T-1133

NUCLEAR REGULATORY COMMISSION

ORIGINAL

In the Matter of: ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON AC/DC POWER SYSTEMS
RELIABILITY

DATE: September 8, 1982 **PAGES:** 1 - 318

AT: Washington, D. C.

TR04
[illegible]

ALDERSON AR REPORTING

400 Virginia Ave., S.W. Washington, D. C. 20024

Telephone: (202) 554-2345

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
SUBCOMMITTEE ON AC/DC POWER SYSTEMS RELIABILITY

Nuclear Regulatory Commission
Room 762
1717 H Street, N.W.
Washington, D. C.
Wednesday, September 8, 1982

The Subcommittee meeting convened, pursuant to notice, at 8:30 a.m., Jeremiah J. Ray, Chairman of the Subcommittee, presiding.

PRESENT FOR THE ACRS:
JEREMIAH J. RAY
JESSE C. EBERSOLE

ACRS CONSULTANTS PRESENT:
WALTER LIPINSKI
E. EPLER
PAUL DAVIS

NRC STAFF PRESENT:
A. KOLACZKOWSKI
ARTHUR PAYNE
P. BARANOWSKI
M. SRINIVASAN
J. MAC EVOY
C. RYDER
MR. KNOX
F. PAULITZ
S. KASTURI
R. BATTLE
J. T. BEARD

DESIGNATED FEDERAL EMPLOYEE:
RICHARD SAVIO

PROCEEDINGS

MR. RAY: The meeting will please come to order.

Can everybody hear me?

Can you hear me now?

Okay. Well, we are all going to have to be cognizant of the fact that at least for the morning session that we don't have any PA system, and I think in our break it would be well to see if we could get it.

MR. SAVIO: I could go up and get the portable unit if that would help.

MR. RAY: I think we should have it.

This is a meeting of the Advisory Committee on Reactor Safeguards, Subcommittee on AC/DC Power System reliability.

Incidentally, is Pat Baranowsky here?

MR. KOLACZKOWSKI: He's on his way. He is coming in on the shuttle.

MR. RAY: We may have to work around him a little bit.

I am Jerry Ray, Subcommittee Chairman. The other ACRS member present today is Mr. Ebersole on my left. It is possible that Drs. Kerr and Okrent will join us later.

We also have in attendance ACRS consultants

Messrs. Epler, Davis and Lipinski.

The purpose of the meeting today is to discuss the status of the NRC Staff's work on DC power systems, and station blackout and matters relating to diesel generator reliability.

The meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act and the Government in the Sunshine Act.

Dr. Savio is the Designated Federal Employee for the meeting.

The rules for participation in today's meeting have been announced as part of the notice of this meeting published in the Federal Register on August 18, 1982. A transcript of the meeting is being kept and will be made available as stated in the Federal Register notice.

It is requested that each speaker first identify himself or herself and speak with sufficient clarity and volume so that he or she can be readily heard.

We have not received any written statements or requests for time to make oral statements from members of the public.

I would ask if anyone in the audience would like to make such a request.

(No response.)

MR. RAY: I would like today to depart from past practices in this respect. It seems to me that this is a subject matter, AC/DC Power Systems Reliability, that justifies participation by industry representatives who may be here today. So if you have any constructive comments or variations in perspective from those which are being and will be presented to us today, I would like you to raise questions or make a contribution verbally.

You are quite welcome to do it, and I firmly believe that we need the perspective of industry in these considerations for possible changes that are probably going to emanate from this kind of discussion.

We have a very comprehensive program. Copies of it, I suppose -- they have been circulated?

MR. SAVIO: Yes.

MR. RAY: We are going to discuss both AC and DC, and update our perspective as well as possibly influence the staff, and we will have comments on what they are proposing to do.

Are there any comments at this point which any members of the panel would like to make?

(No response.)

MR. RAY: Okay, Pat, have you caught your breath?

I would like now to introduce Mr. Pat Baranowski who will initiate discussion of the status of research response work on station blackout. That is Task Action Plan A-44.

(Slide.)

MR. RAY: You are not going to be bothered with a mike at the present time. I don't know whether you like it or not, but this means that you will have to speak out.

MR. BARANOWSKI: No mike. Fine.

I'm Pat Baranowski. I work for the Division of Risk Analysis, for those who don't know me, and I'm the NRC task manager for the unresolved safety issue of station blackout. I'm going to be giving an overview today of the approach taken on this project.

Some of the slides that I have included in my brief discussion here have been presented before, and the introductory ones I will discuss very quickly. I'm interested in particular in letting you know what our philosophy is and how one might resolve this issue as we come down towards the end of our work on it.

MR. RAY: Pat, by way of suggestion, as you do this, we would very much appreciate your pointing out any changes in philosophy that have taken place since you last made your presentation.

(Slide.)

MR. BARANOWSKI: Station blackout is the complete loss of AC power to the essential and nonessential switch gear buses in a nuclear power plant. The unresolved safety issue adsdresses a concern related to are the likelihood and potential accident risks of a station blackout high enough that additional preventive and/or mitigative measures should be taken in terms of licensing nuclear power plants.

Now, although we have defined station blackout as the complete loss of AC power, I should point out that really what we are talking about is loss of sufficient AC power such that the normal shutdown and cooling capability of the plant is impaired beyond what the usual safety analysis shows. So there may be a situation where some AC power is available, but because it goes beyond the normal single failure criterion, we call it a station blackout, namely, because the capability has been impaired.

MR. EBERSOLE: May I ask, maybe at this point I would point out a place where there should be some clarification. There are two possible interpretations of that. You are right that it is the normal cooling methods that are the problem. However, the testing methods and a lot of the words in some of this literature we have here suggests that we associate this loss with the loss of cooolant accident. I wish we would identify whether or not we have adequate reliabiity for the LOCA. I suspect that we have.

MR. BARANOWSKI: The LOCA situation, in particular, the large LOCA, puts heavy demands rapidly on the electrical system. In this issue we feel that a LOCA combined with a loss of offsite power and the loss of on-site power is an event of low enough likelihood that it is not one of concern to us.

On the other hand, the requirements in terms of the number of systems that must function, that is to say, cooling systems, and their AC power needs are the types of things that are used in determining the minimum amount of AC power needed at a plant. In other words, let's take a small loss of coolant accident which is included in the analyses. It requires many of the same systems that a large loss of coolant accident requires, but it doesn't require them as rapidly.

I think there will be some discussion about this as the presentation goes on.

MR. RAY: Pat, I'm a little bit confused. You say the combination of a LOCA and the loss of offsite power and lack of response from the diesels is of no concern to us?

What does that mean from a regulatory viewpoint, and the requirement on the industry?

MR. BARANOWSKI: What that means to me is that the development of requirements for AC power reliability should not be dependent on that type of accident sequence because the likelihood is so low that it is really insignificant in comparison to other accident sequences which would pose a greater risk and should essentially be considered in the design requirements for the AC power system.

MR. RAY: So the evolution of your A-44 effort, in your opinion, should not impose any requirements on the industry to meet this condition.

How about the present regulatory requirements?

MR. BARANOWSKI: Currently the regulations require that analyses be conducted to show that the plant can cope with a loss of offsite power concurrent with a large loss of coolant accident and then take a single failure in any system, including the AC power system.

This goes a little beyond that in that we are taking more than a single failure in the AC power system and therefore combining that with the loss of offsite power and the loss of coolant accident represents a rather small likelihood event.

I would say that that particular issue should be addressed in our final regulatory position. I haven't put that position together. I have a schedule that will tell you a little more about that. I think that would be a good time to discuss that particular regulation, and we would like to address that.

MR. RAY: You will address it in the evolution of your requirements?

MR. BARANOWSKI: Yes. Remember again, the regulatory requirement doesn't call for the consideration of a station blackout with the loss of coolant accident. It only calls for a loss of offsite power, the loss of coolant accident, plus a single failure. In our case, with the blackout, we are usually looking at two or three failures.

MR. EBERSOLE: Just to set the stage for the rest of the discussion, I've got two other questions.

This being the case, if we are looking at the non-LOCA cases as our primary problem, it seems sort of a distortion that all of our tests are the crash start type, which is the LOCA mode of need, which is both damaging and probably unnecessary.

Second, I would like somewhere in the course of the discussion for you to tell us why is it that we seem to have a practice of connecting a nuclear plant to the most unreliable source of power available at the plant, namely, its own output, when we could do a number of other designs to dissociate it from its own output, therefore to make it less dependent on its own output. It seems an absolute distortion to persist in connecting a critical AC generation requirement to the very machine that is going to need it when it fails, okay?

MR. BARANOWSKI: Let me respond at least to the first one. The requirement for the rapid start of the diesels is something that was developed through deterministic applications of licensing criteria, and it is historically imbeded in the licensing requirements. One of the advantages that we have in working with probabilistic risk assessment is that in addition to making engineering judgments based on qualitative considerations, we can also use quantitative guidance in determining what is important and what is worth doing. That is one reason why we selected the reliability and risk analysis techniques to be used in this program, because one has to know where we draw the line, when is enough enough, and where have we missed things that even fairly good qualitative judgment sometimes doesn't allow you to determine the needs for.

On the second item of the reliability of the output to diesel generators, I suspect that has something to do with the economics of running the power plant. I don't know that the effect of using a different source of normal power during plant operation for the on-site systems would represent a great change in risk. I think that is the kind of thing that we would have to look at in developing our recommendations to resolve this issue. If it turns out that that is an important item in the way that the initiator for the station blackout consideration can be reduced substantially, then it has to be addressed.

Today we did not bring our offsite power reliability expert with us, mainly because we haven't quite finalized that report. The reports that you've received or should have received address primarily the on-site power reliability in the accident sequence analyses. Of course, we have factored in what we believe to be the off-site power reliability in those calculations, but of course, they can be adjusted if the final results from that work indicate they should be.

MR. RAY: Is there any representative of industry in the audience who would like to comment on this point, this question that Mr. Ebersole has raised of the power supply system viewpoint?

Would you identify yourself, please?

MR. PAULITZ: I'm Fred Paulitz from Stone and Webster.

The comments that your off-site power is associate with your off-site generator, it is and it is not. As a requirement, GDC 17 requires two other sources of off-site power, independent of each other as much as possible, sharing comming rights-of-way, but not having one line fall on top of another.

In the normal mode of operation of a plant, it is true that you take the power from the main generator to utilize it. The reason is economics in that if you didn't do this, if you passed that, some of these loads are getting bigger, up to about 8 megawatts up through the main transformer, you are paying the penalty through the main transformer and then bringing it back into the plant again from the system, so that under normal conditions they are taking it directly from the generator and stepping it down.

However, when you do have a unit trip, be it the reactor, turbine or whatever, you do transfer it to the so-called independent offsite sources. You do this long before you have to eventually rely on the diesels. It is only diesel generation when you have an unsuccessful transfer or there is nothing there to transfer to, and that is the loss of offsite power scenario, not the tripping of the unit itself.

MR. EBERSOLE: May I comment on that?

Some designs, the Westinghouse being the one I can recall, however, deny that transfer for a period of like 30 seconds, on the grounds that the unreliability of the transfer itself is an unacceptable aspect of that design.

I was pleased to hear that TVA, beginning with Bellefonte, will depart from this practice. So I guess it gets down to how much of an economic penalty this is in the context of whether the additional safety of having an undisturbed source of power is worth it.

MR. PAULITZ: I see a change in some of the designs that -- not the normal power used in the plant but the emergency buses, I've seen designs where they are associated only with off-site power, that they are not required to take the transfer nor the transient nor the problems associated with the normal loads, especially when they are banging on and off.

(Slide.)

MR. BARANOWSKI: Okay. Our approach in this program has been to perform an analysis or an evaluation of AC power reliability which would feed into our estimation of station blackout accident sequence probabilities and consequences, and we would use these results to compare station blackout risks with other accident risks or with the safety goal if that is deemed to be the appropiate item at the time, that we get to the point where we have to make suggestions on how to resolve this issue.

(Slide.)

MR. BARANOWSKI: And we have essentially three aspects of this work that were undertaken over the last year and a half. The AC power reliability, and in particular, the on-site reliability, will be discussed today by members of the staff from Oak Ridge National Laboratory and ADF associates who worked on that, and the accident sequence analyses will be discussed by Sandia. The plant response to station blackout, the hydraulic timing of events was performed for us in this project through the Severe Accident Sequence Analysis Program in the Office of Research. That work has been factored into the station blackout accident sequence analyses and information obtained from that work will be reported by Sandia.

(Slide.)

MR. BARANOWSKI: Very quickly, these programs involve the reliability of the on-site and off-site power systems, the cause, frequency and duration relationships. We are looking at costs associated with reliability improvements, and we are considering what type of AC reliability monitoring should be required by the NRC. Here we would be addressing things like Reg. Guide 1.108 and its adequacy. The accidents sequences, what we want to look at is which accident sequences are dominant from the point of view of probability and risk; how reliable are decay heat removal and reactor coolant inventory control systems during station blackout, what are the dominant factors that influence station blackout accident risks, and of course, the plant response to station blackout.

MR. EBERSOLE: Are you going to distinguish between the various types of plants when you discuss this?

A case in point would be the boiler is notoriously dependent on AC power. The boiler type design is notoriously dependent on heavy AC power to get heat out of the suppression pool. The PWRs can blow it to atmosphere through the secondary system, and therefore they are less dependent. However, GE is now proposing to vent the containments ask a last ditch means of cooling the suppression pool, which puts it in a better position.

Are you going to take these matters up?

MR. BARANOWSKI: The effect of suppression pool heatup during a loss of power condition will be addressed. I don't know if the venting will or will not be addressed, but I suspect the people we have brought here know quite a bit about that particular item and can ad hoc talk about it.

(Slide.)

MR. BARANOWSKI: This is the strategy that has been put together, that is to say, to first determine the current likelihood and level of risk at nuclear power plants to determine if it is in fact a major problem, then make a comparison of those risks, as I have said before, with safety goals or other plant accident risks that we normally accept, and see if they exceed those risks or are less than those risks.

We will be identifying the dominant factors that affect risk. That's the primary purpose of the technical programs, to determine what aspects of design and operation are going to ber important in reducing the likelihood and risk of a station blackout accident. We are looking at both AC power reliability and potential improvements there, as well as the capability and reliability of systems that are needed to cope with an extended loss of AC power.

Given that we understand the important factors that drive risk, we would then propose new or revised licensing requirements which would be consistent with that level of risk and safety goals if appropriate, and hopefully cost effectiveness.

Now, it turns out that the work that we have done indicates that you can't just classify plants by their NSSS or by a couple of simple characteristics of design or operation, but there are a spectrum of factors in design and operation that are important and can change the risk potential from plant to plant considerably.

Therefore, it will be necessary for us to develop a plant specific implementation plan, one that recognizes the weaknesses and strengths, or at least gives credit for those types of things as proposed regulations are implemented so that we don't have either overkill or underregulation as some backfits may be required.

(Slide.)

MR. BARANOWSKI: Licensing requirements, when one looks at cost effectiveness, will involve several technical areas, and in particular the areas that appear to be less costly and give a greater return per dollar involve things like possibly LCOs, tech specs, surveillance requirements, revising procedures for testing, maintenance, and emergency operations, and then lastly, one has to look at hardware capability or configuration.

Obviously someone cannot meet a risk goal through some of the easier to implement types of improvements which may be procedural in nature. So one has to consider hardware modifications. I recognize that the NRC has a large program ongoing now in severe accident research to take a look at how one should consider degraded core accidents and if there should be some revisions to regulations. It is a rather large program. It is rather comprehensive. And because of that, I wouldn't propose that this particular program develop requirements that are extremely expensive unless the risks were shown to be rather obviously large, that is to say there will be a substantial amount of work done in the next couple of years of a much more thorough nature than even this project, looking at all accident risks, and there are competing risk considerations. There are ways to design systems to cover many different types of accident sequences, and before one spends an inordinate amount of money on a particular item, it should be determined that it is effective and necessary to preclude as great amounts of accident sequences as possible.

MR. EBERSOLE: Are you saying in an indirect way that it is not very smart to attempt to be perfect on a small aspect of the safety problem when you can go to something like dedicated shutdown heat removal and cure a lot of ills at a lot less expense?

MR. BARANOWSKI: Right. We are looking at 10 or 20 percent of the problem in terms of risk here, and there is no sense in putting a large amount of effort into reducing that because I will still have 80 percent left.

MR. EBERSOLE: How arel you going to do that when the industry operates on a fragmented basis like it does, and we regulate it on a fragmented basis, and we never integrate it or get any designs that go towards this direction since you cannot by policy introduce a concept on integrated safety? Where are we going to get it?

MR. BARANOWSKI: I hope we ae going to get something out of that severe accident research program I alluded to a few moments ago. That is supposed to be an integrated approach, and it is supposed to be looking at all accident sequence considerations such that any revisions to licensing requirements or proposed backfits are cost-effective on a complete risk basis.

MR. EBERSOLE: The regulatory process

regulates what is put in front of us, and it steadfastly refuses to look at integrated improvements. It is not in your scope, and as a matter of fact, it is prohibited, and I see no particular outstanding advance towards these integral improvements.

Are you telling me that there are some oncoming tht I can look forward to?

MR. BARANOWSKI: I think they are oncoming. Whether they are outstanding, time will tell. It is somewhat of a new approach, as you have indicated. In the past it has been an isolated look at various items, but even in this program we are trying to be working this out in an integral matter. That is to say, we are not only looking at the AC reliability but what are the consequences of not having AC power available?

MR. RAY: Pat, apparently I wasn't listening hard enough.

This integrated approach you mentioned, who ios administering it? What portion of the agency? What can we do to get a perspective on it at one of our meetings and so on, and what part do you play in it?

MR. BARANOWSKI: The Class 9 Subcommittee of the ACRS would have cognizance of this particular work. The program at the NRC is an outcropping from the degraded core cooling rulemaking activities that were suggested after Three Mile Island; that and the minimum engineered safety features' rulemaking were combined together into what was called a Severe Accident Research Program.

There is a document called -- like I said, I don't know the name of it, but it is NUREG-0900 in draft. And that document, at least in the first two chapters, describes the philosophy of an integrated approach to taking a look at safety problems at nuclear power plants. My part in that is as head of the Reactor Reliability Section in Division of Research I have programs ongoing under me to address accident likelihood, which will be used to determine where we should look on an integrated basis to making improvements and whether or not the likelihood of accident sequences are higher or lower than the proposed goals a t are the factors that drive them with respect to accident sequences.

MR. RAY: What was the NUREG you referred to in raft?

MR. BARANOWSKY: 0900. I don't know the title on it.

MR. PAULITZ: Is it available?

MR. BARANOWSKY: It's in draft. I don't know if it's publicly available. I know the ACRS can get it. There has been open ACRS meetings on the topic in which some of the approaches and philosophies that are being used in that program are being discussed.

I should also point out that that program is somewhat evolutionary at this time. It started out a year or two ago and people were not quite sure where we were going. I think the ideas are starting to become more consolidated now as to what should be done with that work, and we are getting some interest, not only from the ACRS but the Commissioners, as to where we're heading on that program, because it could be important in terms of the future design of, say, the whole licensing process.

Well, let me, if I can, get back to this one. What I see coming out of this are a set of generic requirements which can be applied on a plant-specific basis. There would be, I suspect, some minimum design requirements. Here what I'm talking about is, if one looks at the various parts of the problem -- the offsite power reliability, the onsite power reliability, and the ability to cope with losses of AC power, I would think that one wouldn't want to have all of his eggs in one basket in terms of relying on any one of those three aspects to demonstrate low risk.

Therefore, some minimum requirement for any one of those items would be developed. On the other hand, one must consider that some plants might have a significantly better onsite AC reliability system than others, and they at the same time, they have a significantly higher likelihood of losing offsite power. And that kind of tradeoff must be taken into consideration.

There are some plants, which I will call special cases, in which we haven't done enough sensitivity analyses to completely include in our technical programs, and they would have to be looked at on a case by case basis. This would be some of the older plants.

Lastly, I think the requirements should be deterministic in nature. I do not personally feel that we have the standards in place now where we an give a reliability goal and just say, go out and show me that you meet that goal. The truth is, you can use various sets of data and modeling techniques and get a fairly different answer in terms of your reliability estimates.

If that was not the case, I suspect that we would have gone out and made some calculations and in about two months said, here's the answer, and then walked away. No, what we need is substantial peer review, because it is still a developing technology as far as nuclear safety is concerned.

Therefore, I would propose that the requirements be deterministic, but with some foundation in reliability, of course.

Lastly, I think we have to recognize that there are other issues and there are system interfaces associated with the station blackout question. We have generic issues associated with external hazards. In particular, people are well aware of the seismic issue and wind problems that can occur at nuclear power plants.

Fire protection is related to AC power reliability, and in particular when one talks about protecting cable-spreading rooms and so forth. And there are support and auxiliary systems which we look at that require AC power or are required to operate in the absence of AC power in order for the plant to see its way through a loss of offsite power accident.

The AC power system essentially spreads to all systems within the plant and we have to put bounds on what we are doing here or else we would be sneaking through a little generic issue hole into the whole plant and determining reliability for everything in site. I haven't totally worked out how we're going to handle that interface, to be totally honest with you. That will have to be something we discuss later. But I just wanted to point out that that is a problem.

MR. EBERSOLE: Pat, I think it's refreshing that you identify your problem with the preface that this is only part of the larger problem. It's rare to see that in any given program because most programs in general think that's the whole program.

I recall, for instance, virtually all of the safety research work was done on the large LOCA for about 15 years. As a matter of fact, reactor safety came to be connected with anything but the large LOCA, and nobody said this was a small part of a large program.

MR. BARANOWSKY: I really hope we're going to change that a little bit here.

(Slide.)

Let's show you what the schedule is for working on this issue. We would like to analyze the contractor's technical reports by October. They are basically input to the NRC, who has the responsibility for drafting a position, a proposed resolution to the issue, which right now we are shooting for doing in November 1982.

We must go before the Committee to Review Generic Requirements in a two-stage process. That will happen in February 1983 initially. Public comment period will be over in June 1983, since all unresolved safety issues to the best of my knowledge must go out for comment and their proposed resolution.

The resolution of public comments will be incorporated into a final position to be presented before the CRGR in September of 1983. Then the final NRC position should be published in October of 1983.

MR. RAY: What are the present day prospects of meeting the schedule? Do they look good?

MR. BARANOWSKY: Right now I would say it depends on how much difficulty we have with the drafting of the position. Because we are not looking at a simple fix or two, but we are talking about a regulatory criteria that seems to be balanced and fair, it will not be that easy to draft something up.

We will probably have to do some sensitivity studies to determine what can be left out of the position safely. We have not done that work yet, but it can be done fairly quickly. I think that by mid to late November we can have the draft position ready.

MR. RAY: You used the words "balanced and fair" in the regulatory position. Are you in a position to tell us what the response of your management is to that concept? Is it all your idea at the working level, or from a policy viewpoint do you think it has acceptance?

MR. BARANOWSKY: I think it has acceptance from my management. I cannot speak for management in other divisions. If there is someone from Reactor Regulation who would like to address that, I think that is fine.

MR. RAY: Is such a person here?

(No response.)

MR. BARANOWSKY: At any rate, it's not the first time I've made those kind of statements. The approach to resolving this issue has been really laid out in the past before. I think the only difference is we recognize that there is a greater need for the ability to recognize subtle differences between plants.

Now, obviously when the costs are trivial then there is going to be some homogenization of requirements. But I would not suggest going and putting a diesel on every plant because one plant happens to have a poor design.

MR. PAULITZ: I am glad to hear that everybody is not going to get homogenized.

(Laughter.)

MR. PAULITZ: I'm glad to hear the fact that people are recognizing that integration is a problem in the total plant in all systems. I think the biggest problem you are going to have is, in your generic interfaces is the section on interaction. You are going to find interactions between AC and DC going in both directions and all directions, and between all systems and supporting systems.

And if you look over the, what is it, 169 LER's which somebody put out here recently as precursors to core melt, you will find a large majority of those, if you analyze them deeply, and I mean down to the bottom cause, you will find that they are forms of interaction and they've been there for years. And a lot of this interaction has been between safety and non-safety, and it's not been recognized as such, even lately.

MR. BARANOWSKY: Yes. When it comes to interactions, unfortunately that is going to be the type of thing that takes a substantial amount of industry work, because the NRC cannot possibly in its own offices determine the interactions that exist at a particular plant without substantial design information, for instance. And that is an area which we would probably handle by saying: we have identified the following types of interactions as being potentially important; determine if you have these, and if you do make a correction such that they do not occur under the conditions that we've described.

I do not think that there is any one fix-all that we can put in on interactions. They are really plant-specific, especially talking about AC-DC power, configuration of distribution systems. They vary considerably from plant to plant.

Well, I've taken up too much time. Are there any questions?

MR. DAVIS: Yes, I have one. In your discussion, Pat, I didn't notice any indication that you are also using information developed from other NRC programs. And I am particularly thinking about some data summary reports that EG&G has prepared on diesel generator failures. I haven't read all the literature on the subject. I suspect no one has. But EG&G has put out two reports now on diesel failures, and they apparently are working from the same LER that you are, but they're arriving at different conclusions.

For example, I think when you talked to us last time you said there was no evidence that the testing interval has any significant impact on reliability. But in the EG&G report, NUREG/CR-1362, they show about a factor of three to four change in reliability as the test interval is changed from say five weeks down to one week.

There is also a recent report out on common mode failure from EG&G, and there they sort of hedge the final result by saying they couldn't determine the number of demands that were on the diesels because such information was unavailable. And yet, I see some pretty good demand information in reports you're putting out.

I'm wondering why these discrepancies exist and if you're really using all the information that's relevant.

MR. BARANOWSKY: In fact, I would say we are really one of the few groups who is using all the information. Unfortunately, most people are publishing incomplete analyses, such as the EG&G work, which is really an LER summary and analysis of LER rates. We are looking at diesel generator failure rates. We've taken the EG&G work which they've done on common cause failure. We have used the same LER's.

We also asked the utilities to supply us information on the number of demands to take a look at certain LER's that appear questionable in terms of whether or not there was a failure and whether we were interpreting them correctly. And all of this has been analyzed and what you see in the results that we present I think represents a more comprehensive assessment than any of the reports that you have cited.

We are using some of the techniques EG&G developed on common cause failure. We are using those.

But we are using our own quality edit of the data, you might say, which I think is a little bit more comprehensive than what the EG&G people were able to do, recognizing the time and resources they had available. And I believe that will be discussed to some extent by the people either from Oak Ridge Lab or JDF Associates, who have done this work in their presentation.

MR. KASTURI: My name is Sonny Kastouri from EDS.

In looking at your schedule, in the past we have gone through these generic issues and identification of concerns, perceived, probably real, whatever way it is, then come up with some point X where the staff says, here are some of the problems and here is some of the guidance for the industry to work with. Then we get about a month or so to comment.

So in all the time, the year or so it took for you to finalize the industry participation or awareness and identification of the concerns, they had not been taken into account and it's caused us a lot of grief, both the staff, the ACRS and industry at large. Some of the issues that come to my mind is the EQ issue and the SPDS, the safety parameter display system, and so forth.

Could you expound? In what form or shape do you expect to relate your concerns and work with the industry in developing the solutions to the approaches? Or really, you can identify if there is a concern, because oftentimes it's hard to segregate between real and perceived concerns.

What do you have as plans and what does the ACRS Subcommittee intend to do in this area?

MR. BARANOWSKY: You first.

MR. RAY: I would like to make sure you understand our role in life. We don't dictate requirements. We review the actions of the staff and comment to the Commission by way of letters or memoranda, and that therefore goes to the management of the staff.

From our viewpoint, we are an Advisory Committee. We are not the regulatory agency, nor do we have the legal authority to regulate. But we can be very critical and we have been critical, and any action that critiques, if you will, advises the Commission as to the adequacy or inadequacy of new developments, must be a full Committee act.

That is our position. But don't misunderstand me. We'll shoot holes in anything where we think it isn't a fair position.

MR. KASTURI: I understand your role, but I believe, though, that your role is perhaps -- will not be complete unless you have received the input, not only from the regulators, and also from the licensees who have the responsibility for designing and putting in these systems, and if they really identify themselves with the concerns.

My own difficulty has always been, there are a set of perceptions, there are a set of real issues, and I think we ought to separate those things. And we haven't done very well in the past, and in order to do that are you planning to seek industry input? In what form?

MR. RAY: You understand that the law requires that the staff seek industry viewpoints. There's a commentary period.

One of the things I thought you were going to make is that 30 days was not adequate.

MR. KASTURI: I kind of made that point by simply saying you're talking about dropping a bunch of requirements and then giving the public a comment period of one month.

MR. BARANOWSKY: Could I address that a little bit?

MR. RAY: Just a moment. There's a piece here hanging in midair. That is participation by industry.

Friend, I'm from industry, 39 years in industry. So I am blessed, if you will, or handicapped, depending on which side of the fence you're sitting on, with an understanding of your position as an industry representative. I'm completely sympathetic with it.

And since I've joined the ACRS, I've been very pleased to see that this does represent the viewpoint of the majority of the members of the ACRS. They want industry participation. And having come from your activity, I think I can take the liberty of critiquing a position of the industry.

I don't think the industry is as critical of the requirements that are laid down on it as they should be. My indication or my comprehension of the response is, let's not make waves, if that's what they want let's give it to them in order to get on. And as long as that is the attitude -- I may be wrong on this, but this is my perspective at the moment. As long as that's the attitude, you're just going to multiply your problems.

When you have by precedent challenged something and made it a really significant challenge and contributed a better position, better solution, when you've created a few precedents like that, you will get a better regulatory attitude toward you. By "you" I mean the industry.

I think I can take the liberty of criticizing the industry responses because I was there. This is a perspective you might consider.

MR. KASTURI: I think I might also point out that the industry has evolved from a high regulatory era to an era of sort of more working in concert to identify problems. I as an individual can cite several areas and issues where we have precisely in these last few years taken strong stands against regulatory positions and offered constructive comments and are working with the other side of the fence to resolve these issues where they really exist.

MR. RAY: I think that cooperative attitude is what the public needs on the part of industry and regulation. And I do see an improvement, as a credit to Pat and others, in responsiveness among the staff components in this respect. I won't say it's as pervasive as I would like to see it, but I see response.

I think it is important to the interest of safety and economy that the talents that are in the industry from a design and technical viewpoint be applied to the solution of problems on a deterministic basis, if you will, instead of, well, we'll just give them what they are requiring of us and we'll apply our engineering talents to the design to meet that. The technical capability in the industry is a public resource, whether you like it or not, and it is in the best interests of the public that it be used.

You can have the ball.

MR. BARANOWSKY: I don't have too much to add to that. I do agree with what you said. For one thing, it's not clear who the industry spokesman is. Is it a single utility, is it EPRI, is it NSAC, is it NREP? Will somebody tell me?

We have had people from ANS come forward, particularly the ANS Standards Committee, and say, we would like to be cognizant of what is going on here on this station blackout business. They are cognizant, they know what's happening, we are keeping them informed.

In terms of our schedule, we are publishing some reports and we're going to try to make them available in roughly October, which will say, here is what we think the problem is, we are talking about a final issue a year later. We are talking about a public comment period in the June -- in the summer of 1983. The minimum of that comment period would be 60 days.

However, the issue should have been well laid out beforehand and available to anybody who wants them through published NUREG's.

MR. KASTURI: I think I'd like to make one other point. I'm a little bit surprised that you said you don't know who the industry is.

MR. BARANOWSKY: I know who the industry is. I want to know who the spokesman is.

MR. KASTURI: I think we've taken the lead in terms of licensing matters. I don't see why that's --

MR. BARANOWSKY: My name is Patrick Baranowsky and they can contact me any time on this.

MR. RAY: In the same spirit, I would like to make it clear that any members of the industry who wish to submit written comments on the proceedings of this Subcommittee today or at any other meeting are absolutely free to do that, and we will use these commentaries and any questions that might be pertinent thereto in forming agendas for subsequent meetings. So you have a forum in which your viewpoints can be presented both for consideration by the ACRS as well as the staff.

And Pat, while we're at it at this point, it seems to me an appropriate point at which to make a comment. I have been impressed from the beginning of your work on A-44 with the objectivity that you particularly and your team has shown in approaching the problem. I think it is exemplary.

MR. BARANOWSKY: I don't have any further comments on the introductory section here. So if there are no questions, we can get started with the presentation by Sandia. Allen Kolaczkowski from Sandia National Laboratories will make the presentation on accident sequence analysis work that was performed in this program.

MR. KOLACZKOWSKI: Good morning. My name is Allen Kolaczkowski. I work for Sandia National Laboratories. As Pat pointed out, this morning I'm going to be talking about our portion of the program plan for resolving the unresolved safety issue under which the Task Action Plan A-44 is operating.

Basically, what I want to do this morning is take you chronologically through the program as we developed it from its early stages in which we gathered preliminary information regarding station blackout, and grew from that position into essentially the results and eventual conclusions of our portion on station blackout.

(Slide.)

MR. KOLACZOWSKI: As it states, the objective of our portion of the work was to essentially provide the accident sequence analyses and risk perspectives to resolve the unresolved safety issue A-44. We were to essentially focus on three areas, the factors that limit shutdown heat removal under station blackout conditions; identify the dominant blackout accident sequences, their probabilities, provide some risk perspectives; and compare, where possible, with the proposed safety goals; and then to look at ways that the risk could be reduced from station blackout either by design configurations that already do exist in some plants as well as possibly some future considerations which might be applied to future designs.

(Slide.)

MR. RAY: Allen, I'm a little confused. This seems like an explicit statement, but how practical it is is a little bit vague.

In determining the sequences, will you be influenced, or have you been influenced by experience in the industry, or is it strictly an academic determination?

MR. KOLACZKOWSKI: We have made use of the actual experience, what has happened, and tried to factor that in to the analyses where it is appropriate, such as investigating certain portions of the accidents happening and so on. That has been factored in.

MR. RAY: Thank you.

MR. KOLACZKOWSKI: As far as the scope, as Pat pointed out earlier, we feel that through the base case analyses which I will be getting into later, and the sensitivity analysis that can be performed beyond the base case designs, we feel we can cover virtually all of the light water reactors with the exception of maybe some of the very early designs that have some unique features, and maybe those plants that have to be investigated on a case by case basis.

We have looked at external events to the extent information is available. We didn't do any detailed analyses in terms of drawing fragility curves and that sort of thing. We essentially relied on information available and looked at it as it applied to the station blackout issues.

We used the AC system configuration and related data, etc., from Oak Ridge. We will be hearing from that portion of the work in a later presentation.

And lastly, and I think very important, is that we accounted for latest design and operational features since TMI. We did not want to look at how the plants appeared and how they were before TMI. We thought it was very important to factor in the TMI fixes that have taken place and work those into the analysis.

So we went to a great deal of effort to make sure we were analyzing the plants as they exist today, not the way they existed before 1979.

As Pat pointed out, we did take a look at failure to scram and an independent LOCA concurrently with station blackout. Probabilistically, these types of sequences just appear to be very low compared to the sequences you will see later on. We feel that these again, from a probabilistic point of view, are not very important in relation to the other accident sequences which do dominate this issue.

MR. EBERSOLE: Could you tell me how many early PWRs there are and how many BWR 1s there are?

MR. KOLACZKOWSKI: Humboldt Bay, which of course is down, Dresden 1, which is undergoing a considerable amount of change, design change to it, and then Big Rock Point. Big Rock Point, of course, is operating but does have a probabilistic risk assessment on it which covers station blackout.

As far as PWRs, some that are unique and perhaps not covered by these overall generic analyses would be plants like Yankee Rowe, perhaps San Onofre 1, and Indian Point 1. Those are three that come to mind.

MR. EBERSOLE: Is that about the total number?

MR. KOLACZKOWSKI: I would say that was about the total number.

If you look at the entire accident analysis portion of the program, it is divided into five tasks. The first three have to do with essentially gathering information, first from determining knowledge was available when we first started the program, setting up some initial models, and also identifying our interface with the SASA program which Pat alluded to which gave us the accident phenomenology and accident sequence timing information that was necessary. Then we also reviewed past PRAs to see what insights we could gain there -- I'll be discussing those -- and performed some detailed assessments as to the capability and vulnerability of shutdown systems under station blackout. All of this was factored into creating event tree and fault tree analyses and performing the base case analyses, and then through the use of sensitivity analyses, looking at configurations that are different from the base case designs factoring, and again the SASA work and the AC configuration information from Oak Ridge.

MR. KASTOURI: What is SASA?

MR. KOLACZKOWSKI: Safety Accident Sequence Analysis. It is a program sponsored by the NRC.

(Slide.)

MR. KOLACZOWSKI: First I want to talk about Task 1 which essentially involved a critical review of what the state of knowledge was concerning station blackout at the start of the program, our event trees, and I want to point out some unique aspects of the event tree models, and then the SASA program interface.

(Slide.)

MR. KOLACZOWSKI: Regarding the literature review when we first started the program, basically we found that all the information up to that point -- this was up to about a couple of years ago -- was primarily focused on the frequency of loss of offsite power and on diesel generator reliability. There was not a whole lot of information on the plants' capabilities to withstand prolonged blackout primarily because of the existing licensing criteria. That is, you don't have to go beyond the single failure, that kind of thing. There was not a lot of information in that area.

Past treatment of the systems' capabilities and vulnerabilities can be found in PRAs, but we found that the treatment of that was rather inconsistent and hence the need for this program to take a look at that area in considerable detail.

Also, something that came out of the original literature review was that there were some areas that we had to pay some very close attention to. We have talked about interactions a little bit this morning, this being a very important one, that plants do have different susceptibilities, and we couldn't just take a look at one PWR and one BWR and from that draw general conclusions. We found out early we couldn't approach this problem in that way, that there are blackout induced LOCAs which are important to the sequences and probabilities. We had to look at those, and finally, human actions. I think TMI showed us that that could be a very important aspect.

(Slide.)

MR. KOLACZOWSKI: Okay. With regard to the event trees, there are three trees that you will see in a moment. I just want to lead you up to why the three trees, why the number three.

If we take a look at station blackout from a very broad, functional standpoint, we see that in the PWRs essentially we have decay heat removal as a function that remains usually by the auxiliary feedwater system because it is a system that will ontinue to operate and provide heat removal by the steam generators. But we have lost the ability to make up any inventory loss in the reactor coolant system by the HPI system which is AC dependent.

If we look at some of the early BWRs, those with isolation condensers, again the same function remain and are lost in the form of either the isolation condenser or the low-pressure core spray. Again, this is an AC dependent system. If we look at som; of the newer BWRs designs, those with the HPCI or HPCS and RCIC designs, we have interim heat removal and makeup capability via these systems, but we have essentially lost the long term heat removal, such as suppression pool cooling, et cetera, by the use of the shutdown cooling system in the early BWR-3s or the LPCRS mode of the RHR system in the newer designs.

So functionally you essentially have three different classes of plants here, and hence they led to three event trees.

(Slide.)

MR. KOLACZOWSKI: Now, I won't go through this in detail, but there are a few things I want to point out about the event trees. First of all, station blackout, TMB-0 here is the initial input into the tree. All the information regarding that, the way the blackout can happen, probabilities and so on, all come from the Oak Ridge portion of the analysis. That is factored into the tree at that point.

If you look at the tree, one of the unique aspects is that essentially it is a time dependent tree. If we look across the top, you will see the sub 1s, sub 2s, and sub 3s. Those represent different time periods in the accident sequence. The sub 1, this portion of the tree here, we are looking at the ability of the secondary heat removal system to respond to the accident early upon the initiation of station blackout. Also, we are looking at what the RCS coolant system is doing in terms of its integrity, whether the integrity is being maintained or if we are into a LOCA situation, again, early on in the accident. This would be an example of, like, a relief valve being demanded and it sticks open.

Then we ask has AC been restored to the system so we can get out of this accident and respond to it in a successful manner. Given you have succeeded through the initial stages but perhaps have not recovered AC power yet, there are other failure modes that come into play later on in the accident in this sub-2 stage of the event tree where we can get into batter depletion effects; we can get into the fact that we have lost ventilation for a considerable period of time. This could have an effect on the continued operation of the DC systems. Those types of failure modes are investigated in these decision points in the tree in what we call the intermediate timeframe.

Lastly, we eventually ask whether or not AC power has been restored. That is the B-3 event up there because eventually you must restore those systems in order to provide long term heat removal and perhaps containment heat removal, if that is necessary.

MR. RAY: Allen, in your caption sequence, what does TM mean? I can see the others. They identify the sequence of the individual events, but what is TM?

MR. KOLACZKOWSKI: T is the initiating transiet that might be the loss of off-site power or it might be the loss of DC bus, which starts the whole chain of events going. So whatever transient it is, and M is the loss of the normal feedwater or ECS system, and B_0 would be the initial blackout.

MR. RAY: Yes, I realize that.

MR. DAVIS: A question.

In these event trees, have you assumed that manual control of injection systems which are operated by steam is not a viable option?

MR. KOLACZKOWSKI: We have taken credit for manual control where it is possible.

MR. DAVIS: How did you decide whether it was possible or not? I have heard this argument many times and I haven't seen a good conclusion.

MR. KOLACZKOWSKI: We actually were in conversation with, both over the phone and via letter, with people like GE and their turbines and the HPCI-RCIC design, which we call the Terry Turbine who manufactures many of the turbines not only for GE and their BWR plants, but also many of the auxiliary feedwater systems are manufctured by them. So we are in contact with the people who ought to know. We found out that some can and some cannot.

MR. DAVIS: In that same question, have you considered the loss of heat removal from the pump rooms as a problem in manual operation of this equipment?

MR. KOLACZKOWSKI: Yes. As a matter of fact, later on we will see in the HPCI-RCIC designs it is very important or could be very important that ventilation be a factor. We recognize that if the system is responding and running and you eventually use DC power and the guy has to go down and manually operate that system, he is also walking into an environment that might be 150 degrees in that room and he won't want to stay there very long, and that's been factored in.

MR. DAVIS: Thank you.

MR. KASTOURI: What does the CD mean?

MR. KOLACZKOWSKI: Core damage.

MR. PAULITZ: I have one question.

Affecting all these support systems as to how thewy affect all the safety systems, did you consider things like inadvertent operation of fire protection systems damaging the same safety systems which I have seen recently going by, HPCI system got watered down there not too long ago. These interactions, if they are not factored in there, alter the total reliability analysis which goes back to the WASH-1400 concepts and you are going to be missing something.

MR. KOLACZKOWSKI: I am aware of that one in particular. It was looked at.

All I can say is we did what I would like to think is a rather thorough analysis of what potential interactions might be. We think we have come up with the important ones, and we have tried to account for all of the ones we have seen, as we pointed out to Dr. Ray, trying to make use of the experience and the fact that fire water systems could come on inadvertently, that sort of thing, but we are looking at it from a probabilistic point of view. We are asking what is the chance of this coming and the fire protection system coming on also. Maybe that is a factor. It has been looked at.

(Slide.)

MR. KOLACZOWSKI: The second tree, which is basically for the early BWR designs, is structurally identical to the tree I just showed you because again the functions that remain and are lost are essentially the same as the PWR. So it turns out that these structures are identical but the systems represented by the events across the top are different; isolation condenser instead of the auxiliary feedwater. So hence the sequences are different.

MR. EBERSOLE: May I ask one question? Are fire protection systems in particular, they are non-seismic, they are not prepared to cope with common mode failure. Therefore, a seismic incident might isolate the diesel generators because they were expected to be protected individually by CO_2 spray and unusual damper closure systems. For that matter, prolonged loss of AC may trip temperature set points on fire protection systems and cause diesel engines now to commonly spray both drains at the same time, which many of them are designed not to do.

Do you look at these matters?

MR. KOLACZKOWSKI: Okay. Again, as far as the external events, let me repeat. We tried to factor it in. To the extent that information was available, I agree, those kinds of things might potentially happen during a seismic event, but we did not go through and try to in the same detail as we have done here, try to determine what the sequence of events might be during an external event. We do feel we have pointed out what some of the major plant susceptibilities might be in the areas susceptible to seismic events and the things you need to look for.

MR. EBERSOLE: Well, just for a case of AC power failure, do you look at ambient overheating in the rooms within the connotation that you may now trip the fire protection system which is diesel driven and literally wet the whole plant down everywhere?

MR. KOLACZKOWSKI: That is a good point. Again, we have not gone through a mechanistic type of approach in trying to find the sequence of events that would happen during an external event.

MR. BARANOWSKY: Let me add something to that, if I could. The seismic event, for instance, is something that is not just the loss of AC power issue. For that reason, we did not want to tackle all of the things that are associated with seismic problems. That is an interface item that somehow we have to come up with a regulatory framework for handling that as we try to resolve this issue, and if we let things like that become a part of this program, the limits are that we would be doing a seismic analysis on the whole plant, and we could do that with many issues.

So what we have tried to do is identify some problem areas associated with this. We will have to develop a way to treat that interface.

MR. PAULITZ: I agree with you, Pat. If you want to take on that seismic, that is quite a chore, but forgetting that for a moment, just stop and think about if the fire protection system is not designed to the same criteria maybe in the room that it is serving, and if there is one black box somewhere and one single event occurs, let's just say that redundant things aren't going to go down. That's the point. It doesn't have to be seismic. It is just the fact that it is not necessarily designed to the same criteria.

MR. BARANOWSKY: I think we are talking about doing something like a safety versus non-safety system survey as a minimum to be sure that we do not have any unthought of interactions that could exist.

(Slide.)

MR. KOLACZOWSKI: Okay, I just put up the last tree to show you that the newer BWRs, because of the function you have remaining and the functions you lost are different, the basic aspects of the tree are the same, and the time depeniency is shown on the tree.

(Slide.)

MR. KOLACZOWSKI: A few words about the SASA program interface. This is where we got all of the accident timing, sequence timing information, information like how many relief valves are going to open, how many are going to be demanded, that type of thing, how long is it going to take before core uncovery would occur.

As you can see, these are the types of needs we identified of the program. If you take a look at the event trees, essentiall there are three classes of accidents displayed on the event trees, and they are depicted here. We asked SASA to investigate all three classes of accidents. In doing so, we vary these particular items, plant design being things like Westinghouse versus Combustion Engineering versus B&W, etc., and also varying some other items that could affect the sequence probabilities and consequences.

(Slide.)

MR. EBERSOLE: Do you now look at the proposed scheme by the boilers to vent the suppression pool as the final means of rejecting heat?

MR. KOLACZKOWSKI: We said a few words about that in the report. The latest information I have is that although GE was planning on making that part of their standard design, I understand they have done a turnaround on that, and now they are not planning on making that part of the standard design. You will see that does not become an important factor because we have determined that in station blackout accidents, probably the core is going to undergo considerable damage long before the containment is in jeopardy, and we will come to that later.

(Slide.)

MR. KOLACZOWSKI: The next few slides in your handout are some examples of the kind of SASA information we have obtained. I don't think it is worth going through those. It just depicts some curves and sequences of events, detailed sequences of events like finding out how many valves might open. I don't think it is necessary to go through that unless you have a specific question on that.

MR. PAYNE: Arthur Payne from Sandia National Labs.

I don't know if you're aware of it, but that SASA report both on BWRs and PWRs, are published by EG&G Idaho. They are available. I don't know what the numbers are, but they are NUREG documents.

MR. KOLACZKOWSKI: The BWR one is from Oak Ridge. Ron might be able to say something on that.

MR. PAYNE: I think they are referenced in our report, in the main report. If anybody wants we will give you the numbers on those.

MR. KOLACZKOWSKI: A few words about Task 2 which had been looking at published probabilistic risk assessments and what information we could glean from those, and I will address that for a few minutes.

(Slide.)

MR. KOLACZOWSKI: At the time we started the study, these were essentially the PRAs available to us that were published, although I might add, because Sandia National Laboratories has taken an active role in the IREP program, the Interim Reliability Evaluation Program, we were in constant communication with those people and factored that information in and relied on a lot of their data or data in this program.

This is broken down into PWRs down to here, and then BWRs to here. You can see the study on the left, the plant that it was involved with.

There are a few things I would like to point out with regard to this PRA summary. First of all, using our nomenclature for the sequence of events here, you will notice that in past PRAs, among all the PWRs, the one dominant sequence, the one sequence which was found to be dominant concerning station blackout was the $TML B_1$ sequence which has to do with an early failure of the steam-driven auxiliary feedwater pump and then you don't recover AC power in time to prevent core uncovery.

The second thing is that the containment failure modes are essentially driven by either overpressure or hydrogen burn, and that by the way containment failure mode probabilities were all assessed as 1.0 for this kind of scenario. In terms of the percentage of the total core damage probability that station blackout represented or in total risk, you can see it varies considerably. This was the first hint to us that maybe there were important design features that made blackout either important at a plant or not so important at a plant.

Among the BWRs, you can see that there is a little less consensus on what the important accident sequence is. Again, though, they all agree essentially that the overpressure predominantly is the important containment failure mode, again assessed at 1.0 for station blackout, and again, some disagreement as to maybe how important station blackout is. Again, that might be due to plant design differences.

MR. RAY: Allen, were these PRAs undertaken by the utilities?

MR. KOLACZKOWSKI: No. The IREP, of course, is an NRC sponsored program. The reactor safety study, you are familiar with tha. RSSMAP was a study conducted primarily by Sandia of four plants. You see three of them here. The fourth one has just recently been published on Calvert Cliffs. That was an NRC sponsored program. But the ones that are industry are indeed industry identified.

MR. RAY: In the cases were the industry conducted the PRA, is the measure of contribution to core damage probability in the two columns on the right the industry's measure?

MR. KOLACZKOWSKI: Yes.

MR. RAY: It is not an interpretation of the PRA results?

MR. KOLACZKOWSKI: It is our interpretation, although this percentage (Indicating) is really straightforward, it is the ratio of the core damage probability sequences against the total core damage probability. That is a direct calculation. There is not any interpretation involved.

The risk is a little bit interpretive in that basically what we did to get this number was say that risk is dominated essentially by the first three release categories and then the ratio of those versus the other sequences in those categories.

MR. RAY: What I am reaching for is a feel of whether or not the industry agrees with those two columns.

I gather it is so straightforward you would expect them to?

MR. KOLACZKOWSKI: Yes. I have been in conversation with the GE representative recently. We got to talking about the BWR 6 design and they thought that station blackout was a considerable portion of the risk on that design.

MR. RAY: Thank you.

MR. EBERSOLE: In the cases there that catch your eye, where the 30 percent risk appears, and 25 percent risk, did you find that industry reacted to that by saying well, that is a rather substantial number, let's look at see whether we can do something about that for $200 or $300 or $10,000 or $1 million, and respond to it in a constructive way, in short, look at the costs of an improvement in an obviously needed area?

MR. KOLACZKOWSKI: Maybe some of our industry representatives could say something on that. In the particular PRAs, like if you were looking at Limerick or maybe perhaps the RSS-1, I did not see a lot of that in the PRA in terms of the person doing the PRA going back and looking to see what sort of things they could do.

MR. EBERSOLE: I was impressed for instance by the Zion studies which shows that one of the predominant seismic risk is the pendant type pump swings all over the place when you subject them to a seismic upset. So the cost of a few clamps or braces is all that is needed to fix that, but there is no expression that in fact that will be done.

MR. KOLACZKOWSKI: I can't address how industry is planning to use their own PRAs.

MR. DAVIS: One comment on this table. It might be a little bit misleading because the risks that were calculated from these studies were not all the same, obviously. In fact, the Zion risks are like a factor of a thousand below Surrey, so that the percentage of risk you see in the last column is a percentage of vastly different numbers, which means a plant blackout for some stations has a much more significant risk impact than it does for others, independent of those percentages in the last column.

MR. KOLACZKOWSKI: That's true. These should not be directly compared with each other. There were different methodologies, different people performing them, different data was used, and you shouldn't try to draw direct comparisons between items on this page.

MR. DAVIS: The concern I have is that you might say well, since it is 30 percent, that something must be done, but that is not necessarily the case because some of the risks are already so low that 30 percent is an insignificant fraction.

MR. RAY: That's a good point.

(Slide.)

MR. KOLACZOWSKI: The next slide I have just discussed the conclusions drawn from the PRA study.

Task 3, because we saw an inconsistency in the treatment of capabilities and vulnerabilities of a plant to withstand a prolonged blackout, we went to a considerable effort to review essentially shutdown cooling reliability under station blackout conditions. I want to talk about the scope of the features we looked at, the types or examples of some of the systems information and interactions covered, what information sources we used, as I pointed out, examples of the information obtained, and some important insights that came out of this portion of the program.

(Slide.)

(Slide.)

For instance, what we have essentially covered is decay heat removal and reactor coolant system makeup systems, and the support systems for those. That would include things like ventilation, cooling, lubrication, lighting in the room, that kind of thing. Also, the systems and components affecting the integrity of the reactor coolant system under station blackout. This is primarily in the areas of safety relief valve demands, of isolation of the reactor coolant system, and finally of potential leaks in the systems, such as in the pump seals.

Containment systems were looked at, the availability of control room indications and control capability, and then finally procedures and human actions that might be important.

(Slide.)

This is sort of a block diagram indicating essentially the types of information and interactions that were covered in the review of the plant's capability to withstand blackout. For a particular system we gathered this kind of information and also looked at interfaces, that is common modes with other systems, what sort of power requirements were needed, the support needs, as I pointed out, important human interactions, and not only in the initial startup of the system but also later on under prolonged AC loss, whether the operator has to intervene for control of the systems. Those are the sorts of things we looked at.

(Slide.)

The AC-dependent systems were much the same, so I won't go through that.

(Slide.)

You probably cannot read the words across the top here. Basically, this was an illustration of the kinds of information sources that were used. Again, I want to stress the fact that we tried to get as current information as we could, so that we were looking at the plants as they exist today, not the way they existed prior to TMI.

You can see the information sources range from things like SAR's and PRA's, and of course the staff input, down to things like the NUREG-0737 responses, that is industry's responses to the TMI action plan: What were they going to, what changes were they going to make in their procedures and/or the design of the system?

We looked at a couple dozen station blackout procedures that are currently being written by utilities right now. There's the LER data summaries referred to earlier, human factor information, our own review of LER's, et cetera. We went on some plant visits and got some first-hand information from a number of plants concerning the issue.

And then down on the left-hand side you see essentially how that information was used, ranging from basic system information, understanding its failure modes and capabilities, all the way down through procedural failure data and timing of accident sequences.

MR. EBERSOLE: What would you say about the QA on your information sources? I didn't see up there schematics and PNID's and flow sheets and all those things which really constitutes the information.

MR. KOLACZKOWSKI: Here it is.

MR. EBERSOLE: Is that a valid representation, including peripheral aspects?

MR. KOLACZKOWSKI: Obviously this is simplified and the report goes into a lot more detail concerning some of the details regarding the system, but yes, we did look at schematics. And in fact in the auxiliary feedwater alone, I think we found something like 18 different auxiliary feedwater system configurations.

MR. EBERSOLE: Did you find problems with QA on the superficial type of information, which is usually what we get looking at FSAR's and PSAR's? These things, you know, you must not assume automatically that they represent the real facts of life. They come from a licensing group and a design organization or a utility, which may or may not have some affiliation with the design team.

MR. KOLACZKOWSKI: That's a very good point. But keep in mind, the SAR's were not the only thing we looked at. In looking at industry responses to particular TMI things, we have exactly what the utilities said they were going to do. They were going to put in this widget or make this operational change, and of course that was also factored in.

MR. EBERSOLE: So you looked at the QA, then?

MR. KOLACZKOWSKI: Yes, I think so. That's just the typical example of the auxiliary feedwater system, two motor pumps, a steam-driven pump leading for steam generators, although, as I pointed out, I think we actually found 18 different auxiliary feedwater configurations.

MR. EBERSOLE: That doesn't reflect that all of these may be sitting side by side in the same room with a sewer pipe hanging over top of them.

(Slide.)

MR. KOLACZKOWSKI: That's true. Again, this is a very superficial summary of the kind of information we were gathering on the systems. You can see here some important aspects regarding the turbine train, the fact there are many trains possible in existing plants today, up to three. They're usually powered by station batteries, but could be powered by dedicated batteries. And there are other items as listed.

The important item here is they are all undergoing the TMI fix to make sure the steam-driven train is truly AC-independent. For instance, that it doesn't rely on some lubrication pump that is AC-powered. Then you see variations on the motor trains. You'll notice that some of them are even powered by a dedicated diesel and battery system. The CST tank from which the auxiliary feedwater systems draws, the time that water source will last can vary considerably, and information on the transfer to a secondary water source once the CST has run dry.

MR. EBERSOLE: That motor train implies that we have standing multiple turbine trains with no motors, with no activity to do something about that. Is that true?

MR. KOLACZKOWSKI: Yes, there are plants that have like two steam-driven trains and no motor.

MR. EBERSOLE: Davis Besse is one?

MR. KOLACZKOWSKI: Well, Calvert Cliffs, for instance, was one. I think they're putting in a motor train now.

MR. EBERSOLE: That is what I was going to say. Isn't there any regulatory pressures now to require motor-driven trains?

MR. KOLACZKOWSKI: I don't know. I can't address that.

MR. BARANOWSKY: I don't know that there are any regulatory requirements for backfitting of plants that don't have motor-driven trains in them. On the other hand, decay heat removal is in unresolved safety issue task A-45. That type of thing should be addressed there. And the people working on that program are trying to follow everything we're doing here, so that there is reasonable continuity.

MR. KOLACZKOWSKI: Again, with the information you gather on these systems, you can then determine its potentially important failure modes. This is just an example of a very simplified fault tree.

Recognizing the fact that, depending on the time frame I was talking about earlier in the event trees, the auxiliary feedwater system is susceptible to different failure modes. During the initial starting during the early time frame, we see the turbine hardware failures and TNM failures and so on coming into play; whereas later on in the DC power depletion could be an important factor; and then finally a continued water source is necessary in order to keep providing decay heat removal.

(Slide.)

MR. EBERSOLE: One design is currently contemplating requiring a 10^{-4} failure per demand for the ADF auxiliary feedwater system as a design basis. These are Combustion that don't have PORV's. Is there any evidence that has come out of studies that shows that this is a practical goal or not a practical goal, or can you comment on that? That's 10^{-4} per challenge.

MR. KOLACZKOWSKI: I really don't think I can comment on that. I think again that kind of question might be better addressed by the people working on the overall decay heat removal procedure in the Task A-45 program.

MR. PAYNE: Arthur Payne, Sandia Lab.

It depends on what event they're responding to. 10^{-4} for every event, including loss of offsite power?

MR. EBERSOLE: 10^{-4} is a generic

requirement. They do not propose to have any method for putting water into the primary loop by virtue of having now PORV's at all.

MR. PAYNE: Is AC power going to be available? Is 10^{-4} even in the case of station blackout?

MR. EBERSOLE: I don't know.

MR. BARANOWSKI: I don't think they are talking about to the 10^{-4} in the case of station blackout. They're saying, given an initiating event, which could be either a loss of feedwater to the mechanical type problems or the grid, for instance, what would be the reliability of providing secondary heat removal. 10^{-4} is possibly a reasonable goal.

MR. EBERSOLE: Thank you.

MR. KOLACZKOWSKI: A couple of items came out of this review of the shutdown cooling system capability, and so on, which weren't necessarily rigorously treated in the quantification aspects of the program, but which we feel are still very important to point out.

The first item, procedures to be detailed for bringing the plant to a safe shutdown even once AC power is restored, you will see later on that bringing on certain containment systems could even be detrimental rather than helpful. It is things of this sort, whether you need to bring on a cooling system, before you actually start a pump on line so that you can provide cooling water to its bearings and so on, those sort of aspects need to be considered once AC power has been recovered.

In some procedures we found this item was treated in a very detailed manner. They went through and tried to logically think out, which systems do we need to bring on line first, which systems can wait until later, what order will we bring things on in, and so on. Other procedures were not nearly as detailed. We think that's an important item.

I've alluded to the second one. Station blackout procedures do vary considerably in the amount of detail and what they cover thus far to date. As I pointed out, utilities are working on blackout procedures at this time. External events, particularly fire, seismic and wind, could cause station blackout or conditions similar to that -- I'll get to that on my next slide in a moment -- with frequencies in the range shown.

Security systems. We want to make sure that if we've lost AC, and perhaps even later DC power, we want to be sure we can get through the doors so that the operator can manually get down to some remote location and perform manual operation. We want to be sure you can do that, that the door isn't going to sit there locked and you can't get through it.

Regarding any thermal shocks to the reactor coolant system, we essentially made an assumption here, which is backed up somewhat by SASA analyses, that is if cooling is restored before there is significant core damage, we feel that any resulting thermal shock to the system, be it the piping, the steam generator tubes, the vessel itself, we don't think will result in failure of a large enough magnitude to be of a concern.

Two-phase flow in the PWR, the SASA analyses and the TMI event itself show that two-phase flow will occur before core uncovery, but it is reversible. You can get back into the solid-type regime.

Finally, down time due to test and maintenance may be abnormally high on some AC-independent systems. We found this particularly true looking at tech specs on a few of the early plant designs, where the auxiliary feedwater system was not considered as, shall I say, as safety-related a system as it's now considered today. And also, in the area of the isolation condenser we found that some of the tech specs allowed for a considerable amount of downtime.

MR. EBERSOLE: Is that first paragraph scoped to include AC power outage long enough to have lost the batteries?

MR. KOLACZKOWSKI: The first item?

MR. EBERSOLE: Yes.

MR. KOLACZKOWSKI: Yes.

MR. EBERSOLE: And therefore you do have a presumed procedure to recover from loss of batteries?

MR. KOLACZKOWSKI: Yes.

MR. EBERSOLE: That presumes you have some way of sustaining loss of batteries and you still know what is happening. By what source of power do you get your intelligence?

MR. KOLACZKOWSKI: We'll get into that in a little bit more detail. If I could delay that question until a little later, I think that will come out.

(Slide.)

Just a word on external events. I think it is very -- it is very plant site and plant design-dependent. If you look down the left at the various events which we think are the more important ones concerning station blackout issues and you look at the plant's susceptibilities to those events, you see things -- like in the seismic, one of the more susceptible areas of the plant is the switchyard. If the seismic event is of sufficient magnitude and lasts long enough, there is a very good chance that you are going to lose off-site power. So you've got the initial stages of this event because of the initiating event.

Also, you may lose control capability, because again, depending on the magnitude and the length of the event, relays can start chattering, that sort of thing. So even though the diesel generators themselves may be operating, you might not be able to control the system. So as far as the system is concerned, it looks as though it's a station blackout because you can't get the power to the system to be able to control it properly. So you may not have a station blackout per se, but the plant response is very similar as if a station blackout had occurred.

And of course, your non-seismic systems are your next most vulnerable areas of the plant. Similarly with the other ones, you see things like the grid towers, the switchyard, and in the case of the fire and floods you see, wherever there are areas where there are multiple divisions coming together such as in the cable spreading room, and so on, these are susceptible areas that can make the plant response to these events look like a station blackout, although it may not be a blackout per se.

Again, in summary, based on some of the information we have at this point, and not doing a detailed analyses in those areas in this program, it appears as though current estimates range in this order of magnitude for potential core damage probability due to these external events.

(Slide.)

Now I want to get to the two results tasks, where we actually put our generic models together and performed the analyses. I want to talk about the fault tree development a little bit, where we got our data information from, the key post-TMI changes factored into the analyses, why there are four base case analyses, why they were performed, why there were four, compare those results with the proposed safety goal, and then talking a little bit about sensitivies for looking at other design configurations that are different from the four base-case analysis, so that indeed you can look at a station blackout issue for a specific plant, then finally provide some containment failure insights to add a risk perspective to the entire analysis.

(Slide.)

This is sort of a simplified diagram of the basic structure of what the fault trees look like. For each system examined, we look at the independent failures of parts of the system, as well as combinations of failures and test and maintenance outages and common mode failures.

For each failure, essentially the fault tree was broken down so that things such as the human-related failures, such as maybe failure to initiate a system or something like that, was factored out separately. The power requirements were factored out separately. The other support systems were factored out separately in the tree likewise.

These little house gates, these were things we could turn on and off in the tree to essentially look at different design configurations, such as this might be a single steam-water-driven configuration and this might be a two steam-water-driven configuration. We could turn on and off those basic configurations and look at the system reliability.

(Slide.)

A few words about data. We used a lot of sources to get data information for the program. You can see they range from PRA's, including the IREP analysis which was going on while our program was going on, generic feedwater studies performed by the NRC, industry responses to TMI action plan items, data summaries, et cetera.

We critically reviewed that data to make sure it was currently applicable, so that, for instance, we weren't -- so that we would rule out failure modes of the auxiliary feedwater steam-water driven train due to AC dependencies. We ruled that failure data out because now, after post-TMI, supposedly the plants are making sure that those dependencies don't exist. So that type of failure data was taken out of the entire data bank used for this program.

We used representative generic values for the base case analyses. The point I want to make here is, we are not doing a worst case analysis in terms of reliability of the individual components and systems.

As far as human errors, a few words I should mention here is that the available information sources we have on human error treat very well the recurring human error type of event, where maybe the guy is supposed to go down and test the system and then he may leave a valve in the wrong position. That type of thing is treated very well.

What is not yet treated very well in the data sources are, given some accident situations, some set of indications, what is the chance that the operator is going to make an error then in a one-time situation? So we had to rely to some degree on engineering judgment here, although where we could we made use of data sources like Swain's Handbook, like PASS. And basically, I have categorized the kind of failure probabilities that were used for the human errors in the fault trees depending on the specific considerations you see here.

Finally, the blackout likelihood and the AC recovery potential. All that data and information came from the Oak Ridge portion of the program, which will be discussed later.

MR. EBERSOLE: May I ask a particular question that occurs to me from having looked at a new boiler that is being built? This particular plant had an interesting standby coolant system which had been designed with rather sophisticated interlocking arrangements.

I noted that they had a required interlock that the coolant pumps be never started if the valves were open, because the pumps would go to runout and therefore presume to be damaged and the motor burned out. To start with the valves closed raises the question, the lines are not filled and it may cause a water hammer.

Do you look at this degree of detail in your studies? Is this a generic characteristic of pump valve configurations?

MR. KOLACZKOWSKI: I think there are particulars like that that are very difficult for generic programs such as this to try to cover. We did look at, for instance in the BWR's, they do have this fill system which is typically supposed to keep all the water lines filled with water.

MR. EBERSOLE: Some water lines.

MR. KOLACZKOWSKI: That's right, like in the core spray pressure system and so on. You'll find that that's not so important because, as you'll see later on, it turns out the recovery of AC power in the first place so drives this problem that a lot of those things really don't become important to this particular issue and we didn't have to get into those details, it turns out.

MR. EBERSOLE: Thank you.

MR. KOLACZKOWSKI: Important post-TMI changes. Really, the more important ones that were factored into the analyses. I mentioned the TMI fixes concerning the auxiliary feedwater system, making the steam-driven train truly AC-independent, that restart of the reactor core in BWR's being made automatic. In other words, once it ran it would shut off.

Relief valve. There's been a considerable amount of work, a lot of work going on making sure there is adequate indication and alarm status and control capability even under station blackout conditions. The SPDS system is an example.

Finally, as I pointed out, utilities are writing station blackout procedures. We were able to get a couple dozen of those and look at those and see what kind of things they thought were important and factor that into the analysis.

(Slide.)

Okay, you remember I had three event trees for three classes of plants. The PWR's, as pointed out, essentially have the same function remaining and the same function loss, regardless of the design. So we were able to group the PWR's into essentially one generic plant class.

For the base case design, we took a realistic design, but one that, granted, it's rather susceptible to station blackout because there are only two divisions of shutdown, cooling and emergency power. We also factored in a common service water dependency for cooling of the DG's and the AC pumps. That is, you might rely on the same service water pumps to cool the diesels as well as to cool the bearings on the AC pumps.

Battery depletion time was taken as five hours as sort of an average estimate based on a number of calculations that we have that utilities have performed on how long their batteries would last. Given these conditions and not a large LOCA condition occurring concurrently, a single steam train of auxiliary feedwater, you can see the other things that were factored into the base case analysis.

This is just essentially to get an initial cut at what's importantant in PWR's to the station blackout.

(Slide.)

This nomenclature down below, you'd have to refer back to the trees to see the specific sequence it's referring to. But again, I would point out that past PRA's have said that it was the early unavailability of the auxiliary feedwater system and then failure to recover power which is the important station dominant blackout sequence. That is represented here.

We also found in this study that there are a number of other sequences in the intermediate time frame, the B_2 time frame, that are also important to station blackout. Basically, you see a plot on the log scale sequences, with all the uncertainties factored in on the data and the initiating frequency of event.

MR. EBERSOLE: Was it at this point you were
going to tell us how you got the 50 percent probability
that you'd have the diesel running without AC?

MR. KOLACZKOWSKI: Let me go back to that for
just a moment.

MR. EBERSOLE: I'm just curious as to how you
know what you're doing.

MR. KOLACZKOWSKI: Like this one right here?

MR. EBERSOLE: Yes.

MR. KOLACZKOWSKI: For that particular item,
.5 was really a screening item we used. It was based on
the following information: conversation with people
like Terry Turbine --

MR. EBERSOLE: Suppose I were to say that was
zero. Would it make much difference?

MR. KOLACZKOWSKI: You can see where we can
treat that number now in the sensitivity analysis and
see what affect zero would have.

MR. EBERSOLE: Okay.

MR. DAVIS: Excuse me. What do you use as
your T event probability?

MR. KOLACZKOWSKI: All the initiating event
probability that goes into the tree. That's based on
the two AC system that I talked about, part of this base
design that comes from the Oak Ridge data. We took a

look at the Oak Ridge data here to see what was the probability of station blackout occurring in a plant that had only two diesels. In this case they happened to be service water-cooled. There is a common dependency between the cooling for the diesels and the cooling for the pump on that service water.

All that data came from Oak Ridge in the form of an equation and data and so on that was factored into our analysis. All that came from Oak Ridge.

MR. DAVIS: Where are those numbers, in your report? Do they appear?

MR. KOLACZKOWSKI: Not per se. As far as finding the numbers in terms of station blackout, what's the chance of it happening or what's the chance of it happening and lasting for X amount of time. All that's in the Oak Ridge report.

MR. PAYNE: There is some of that information in our data tables in our report. That is, the initial event failure probability, and there are recovery factors for recovering different types of AC failures. That is in our data section of our main report.

MR. DAVIS: Did you consider repair of the diesel as a function of time?

MR. KOLACZKOWSKI: Yes. That also came from Oak Ridge, in terms of how offsite recovery might change with time, how diesel generator repair might change with time, service water repair, what have you. That was all factored in.

MR. DAVIS: The diesel repair, did they consider the fact that you didn't have any AC power at the time the recovery operations were underway?

MR. KOLACZKOWSKI: I think it would be better for them to answer that question.

MR. BATTLE: Ron Battle, Oak Ridge.

We don't have much data on repair of diesels without AC power, so we took the mean time that we have data on repair. But it's with lights and with normal conditions.

MR. DAVIS: I've seen this also in PRA's, and I have a little concern about whether that data is really applicable, because without AC power you are really going to be hampered in repair operations. You might not even be able to get air to restart them, if you can't get the compressors going.

MR. BATTLE: Well, I'll show you a curve I had on how the dependability changes with time. It includes failure to run time. It's not a big contributor. It's not likely you're going to repair a diesel. There's a fairly long repair time, so you'll get offsite power back. That's the way you'll get AC power back, most likely.

MR. EBERSOLE: Did you find the diesel generator rooms well illuminated with DC lights?

MR. KOLACZKOWSKI: Yes. That's one question we always ask. And supposedly, yes. It wasn't bad; let's put it that way.

MR. EBERSOLE: What was the ill effect of this combined water supply? You imply that that's significant, that the pumps and engines were tied in, that you had to have water for both those things.

MR. KOLACZKOWSKI: You'll see that in just a moment.

MR. RAY: What's the significance of the point value?

MR. KOLACZKOWSKI: Point value is essentially a best estimate, basically just taking the probability as being a best guess and using what we call a rare event. You don't factor in the uncertainties. You factor in the probabilities, and that's the best guess of what the probability is. The rest of this is factoring in the fact that these are all uncertainties on that data.

Okay, the first graph I showed you was for a B&W plant, because there are smaller inventories of water. The probabilities vary a little bit from the

Westinghouse and CE plants. If you were to compare this graph with the former one, you'll find there was really not much difference. The same sequences are important.

(Slide.)

This will answer your question, Mr. Epler, about the service water dependencies as pointed out in here. The first number you see is the mean probability that came off the previous graph for the B&W plants. Then here's the mean probability for the Westinghouse and CE plants for the four important sequences in station blackout.

What's more important than that is the factors that are making those sequences dominant. Again, in the early time frames, as you might expect, things like the initial unavailability of auxiliary feedwater steam water train is important whether or not you can recover power. And as Ron pointed out, really the recovery of offsite power is the thing that really dominates.

In the case of a few plants where they do have AC valves in their letdown lines, it is important to recognize that this dependency solely on AC power to isolate that line could be important and is a contributor in the early time frame. In the later time frames, we see different things coming into play in terms of what causes these sequences to be dominant. Here you are involved with the eventual loss of DC power due to battery depletion, and can the operator still continue to operate that steam driven turbine or not, and of course AC recovery.

Another has to do with the large pump seal failure. Here you are concerned with the fact that you may get pump seal rupture because you have lost pump seal cooling over an extended period of time. You start leaking coolant from the reactor coolant system. In order to run makeup capability systems, you need AC power, so if you have this coupled with still the non-recovery of AC power, it becomes important.

This becomes important in that even if AC power is restored, if perhaps part of the reason the AC was lost in the first place, loss of service water cooling, you couldn't cool the diesel and it wouldn't come on line. Even though you might recover power, off-site power, if that same service water is used to operate or to cool the AC pumps, even though you get the power back, you may not be able to run the pumps very long because of the fact that the service water went down initially as a contributor to the blackout event and you still haven't gotten it back, so that even though you get off-site power back, you can't run the AC pumps very long, because you are liable to overheat the bearings and that type of thing.

So, depending on how dependent you are on the service water and how common it is between the diesel generator cooling and the AC pump cooling, this could be an important factor.

Then, lastly, the CST depletion time, again, AC recovery and whether you have AC dependencies in the alternate water source, in the very late stages of the accident, if you are able to get through these first two stages.

MR. PAULITZ: These common water systems bother me somewhat, in the fact that in the long term we are supposed to be redundant and independent, and what you are telling me is, you are getting figures from some place here. What you are saying could play an important role. I will grant you that in the long term if you don't have redundancy you might get into trouble. Certainly it can't support adequately some other independent systems. They may not be independent. They may be common. But those things -- I don't know where you are getting such systems from.

MR. PAYNE: Let me answer that. The service water dependencies we are looking at, most AC power pumps, for instance, in the high pressure injection system are not cooled directly from the service water system. The service water or salt water cools component cooling water, okay, or the service water system. You have one basic system that cools these other two systems and then cool independent systems. What we are looking at here is not a single failure in the lines to the DG's, but failures back in the common cooling water system which causes you to lose all cooling water.

Now, this may or may not be important. It seems to me personally unlikely that you cannot run HPI pumps with the heat sink that you have in the component cooling water system for a long period of time, but that has not been demonstrated to us that you can do that, so we put in here that if you didn't have the cooling it would fail the pumps. So we said, okay, what if the industry could demonstrate that you don't need a coolant. What effect would it have? Then we did a sensitivity on it and factored it out.

MR. KOLACZKOWSKI: We don't mean that

everybody has a common service water dependency. Again, we are pointing out an area that is important to look at in the eventual NRC look at the role, that just because he has got AC power back, that doesn't mean everything is okay. You have to get the systems operating.

Probably the one other system you could think of that might be common to many systems in the plant is the service water, and if indeed there are some very strong common dependencies there that could also be a contributor to certain accident sequences.

MR. PAULITZ: I agree with you, but the Commission has been after everybody for a number of years to make sure that these ultimate heat sinks are independent and redundant, and if there are commonalities, whatever is going to cause them to go down had better be a very low probability as well.

I grant you if they are there they may play a significant role, but I am wondering whether we are really treating the real world here or not.

MR. KOLACZKOWSKI: I think some of the older plants perhaps don't meet some of the requirements you are thinking of in your own mind.

MR. EBERSOLE: Is this to say that the regulation system has not now eliminated these single dependencies after all these years? I guess I have been living in a dream world. I thought these were being cleaned up.

MR. KOLACZKOWSKI: Well, it is just like the diesels. We have more than one diesel at the plant, but that does not mean that there are not common mode potentials between redundant trains.

MR. EBERSOLE: I am talking about going into the things you referred to and rooting them out. I was very much disturbed to hear recently about a sea coast plant which found out it had a common discharge valve for all the critical service water, which happened to get locked in place. They lost the power to it. In short, this was a complete blockage of all the water from the cooling water systems. I am really not sure that the regulatory requirements had required multiple discharge of safety grade characteristics.

MR. KOLACZKOWSKI: I can't really address that. All I can say is, even in Peach Bottom, they identified a single valve in the service water system that would fail service water cooling to all the diesels and so on, a single valve, so maybe all designs have not been worked out.

MR. PAYNE: Most of the systems we looked at, the failures, the possible failures of the common water systems were negligible. They are down in the 10^{-6}

range. The one in particular that was fairly high was the one --

MR. KOLACZKOWSKI: I said Peach Bottom. It was Surrey.

MR. PAYNE: If they have a single valve, if it is open, it will drain all the cooling water, and you have no cooling water. I don't know if they have fixed that.

MR. KOLACZKOWSKI: I am sorry. It was Peach Bottom.

MR. PAYNE: In the PWR they also have something like that. Now, I would say in general it probably is not a significant problem. Most systems are sufficiently redundant with three or four or five pumps and independent lines feeding a significant number of cooling systems that you don't really have to worry about that, but there is a potential for that in some particular plants.

MR. EBERSOLE: We are so supply oriented to see where the water comes from, sometimes we don't look at where it went, how it was dumping, was there a clear path for it. Did you scope your studies to make sure there weren't common mode blockage valves or single valves like in this plant that recently failed?

MR. PAYNE: That was the idea of what we tried to do, where it is coming from, where it is trying to go, and seeing if there is an impedence of the system.

MR. KOLACZKOWSKI: In this study, we could not look at the service water design for all 70 plants or whatever it is that are out there, but in the limited review we did do looking at the PRA plants, for instance, and so on, we saw this as a potential such as in the reactor safety study, and we thought it needed to be recognized.

Okay, how do you take this b[illegible] case information now which points out the major factors that affect blackout and how do you come to conclusions about specific plants? The way we suggest you do that is through these sensitivity analyses. This is a rather detailed chart here. Let me show you basically how to read it. I will go through one or two examples.

If we take the auxiliary feedwater steam train unavailabilty, here you see the value that was used in the study, which is both the hardware and the test and maintenance contribution. If that train is unavailable when you need it, as a sensitivity, if we vary that unavailability in the range shown, which we feel kind of represents the unavailability that exists out in the industry currently, then we take a look at the sequences that that sensitivity happens to affect the most.

In this particular case, because we are talking about the unavailability of the steam train, it affects B1L1 sequence, that is, the early sequence. Here you see the value. One thing I should point out. These are point estimates. These should not be confused with the mean values on the previous slide. We did this because it is a lot easier to perform the sensitivity analyses on the point estimates because you can do very direct multiplicative type calculations, whereas if you are going to look at the effects on the mean, you have to actually go back through and run through the entire uncertainty analysis again, because now you have taken out a particular uncertainty and that affects the uncertainty analyses on the entire sequence.

However, the effects you will get on the means are close to the effects you get on the point estimates, okay? So what you see here is a corresponding point estimate for this sequence's probability for the B&W plant and for the Westinghouse and CE plants. That is before you apply the sensitivity. If you apply the first sensitivity in which the unavailability increases, then you see we get a corresponding increase in that particular sequence's probability. Therefore, if you have a plant that has a history of a very unrealiable steam water train, and maybe represents more of this upper value in terms of its unavailability, then obviously this sequence's probability would increase.

Conversely, if you have a very good steam water train in your plant and a history such that you have not seen any failures or whatever, then you can get a corresponding decrease of like a factor of ten. One thing to note is that that is the only sequence that this particular sensitivity affects to a large extent. The other sequences, the other three I showed you are not affected by the sensitivity, and therefore the entire core damage probability where this is the value for B&W before and Westinghouse and CE plants before, then you see that if you have a less reliable auxiliary feedwater steam train, that value then goes up some, like a factor of one and a half to two, or it can go down by again not a very significant amount, because this sensitivity is not affecting the other potentially dominant station blackout sequences.

Likewise, we look at auxiliary feedwater two steam trains, not part of the base case analysis. Here is a value for what we feel would be realistic of the unavailability of the two steam train configuration. Again, you see a rather large decrease in one particular sequence's probability, but again not in the others. That happens to be common for most of the sensitivity you perform. You find out you affect certain sequences but you don't affect them all. So, from a shutdown cooling standpoint, there are actually a number of features that you need to address simultaneously before you can get a significant decrease in the overall core damage probability.

Some of the other slides address some of the other sensitivities, like common service water dependencies and what about if you take that to a small value, whether the operator can run the auxiliary feedwater without DC, and so on.

(Slide.)

MR. KOLACZKOWSKI: You can perform combinations of things. Suppose the auxiliary feedwater system, rathern a minus 2 unavailability, it is $4E^{-3}$ and suppose that the battery depletion time, rather than five hours, is 12 hours, and that the seal leak time -- that is, the time it would take to uncover the core given the reactor coolant pumps are leaking because of loss of seal cooling -- if you varied that from a probability of from 5-8 to 12 hours to essentially it would take a day and the CST depletion time has been increased from eight hours to a day, you can take that as a group and look at how it affects certain sequences, and what it does to the overall core damage probability.

Those kinds of changes will give you factors of for instance ten in the overall core damage probability in terms of reduction. You can see that in this way, essentially what you can do is take a look at a specific plant's design. Through this sensitivity analysis, you take at least a first cut estimate on where that particular plant may lie with respect to the station blackout issue.

One thing I would point out is that I think it is no surprise that the blackout probability -- that is, the frequency of off-site power, what is the chance you are going to lose all AC power, and that has factored into it the diesel generator configurations, how many diesels you have, and so on. That is really the dominant thing, because that one thing alone, as you might expect, can make considerable reduction or even perhaps increase if you have a very unreliable AC system in terms of the overall core damage probability. That is really the one factor, as you might expect, that is really important, and it drives the overall core damage frequency.

(Slide.)

MR. KOLACZKOWSKI: I want to go through these quickly. Isolation condenser was the next event tree we talked about. Those were treated as a plant class, although we did break this up into two little subgroups, one using two isolation condensers and then one using only one condenser, but it also has an auto feedwater coolant injection system which is AC dependent for RCS makeup. We just wanted to see whether the one condenser versus two condenser design, whether there was a significant difference in that or not. It turned out there was not.

(Slide.)

MR. KOLACZKOWSKI: For one of the configurations versus the other, this has to do with the unavailability of one or two isolation condensers. You can see the kind of core damage probabilities you get are about the same. Both plants suffer from an early RSC integrity loss and failure to recover power and also a later loss of RCS integrity due to pump seal leakages, and again still no AC power recovered.

(Slide.)

MR. KOLACZKOWSKI: That is demonstrated on the next slide. There are the three sequences that dominate concerning station blackout. The mean probabilities are shown. Again, the factors that dominate. AC recovery again being the one factor throughout. Then we have the RCS integrity loss here as well as here, and that common service water dependency is a factor again.

This assumed there was no independent AC makeup capability, when in fact there are isolation condenser plants that are either adding or have a fire pump, for instance, for RCS makeup, or some plants are adding a HPCI system, which is a DC dependent, steam driven system for makeup capability.

In this case, because of the isolation condenser design, the majority of the core damage probability is driven by loss of RCS integrity, that indeed if you can provide a makeup capability you can look at all the sequences and get an overall reduction in the core damage probability of better than a factor of ten.

MR. EBERSOLE: Throw that previous slide up there a minute, please.

I just am getting a look at these probabilities. They are 10^{-5}, some number times 10^{-5}. When we are up in that area, I guess I have a commitment to ask you about your consideration of common mode failures, and the point of entry of these types of effects. To add a number like that or even slightly lower, are you convinced that you look at the contribution of common mode influences thoroughly?

MR. KOLACZKOWSKI: I think so. Certainly in the AC work. I think they tried to do it in terms of looking at the diesel and air start system, and so on, those kinds of configurations. I think that has been looked at from their point of view. From our point of view, as I pointed out during the review of the systems, we tried to account for the operator potentially being in a common mode. At the support system, common service water, lighting in the rooms, those kinds of things, we went through precursor information, historical experience, looked at where and what types of common modes have been occurring, and then tried to account for those in our analyses.

I think we have done as good a job as can be done.

MR. EBERSOLE: Thank you.

(Slide.)

MR. KOLACZKOWSKI: If we look at the newer BWR's, remember, that was the third event tree. Here, we made a distinction. We took the newer BWR's and broke them into two subgroups, those plants typical of the BWR four vintage, which have HPCI and RCIC systems which are two independent steam driven pumps which provide both decay heat removal and makeup to the reactor coolant system, then the BWR 6 design, which has essentially the alternate decay heat removal concept. It has the HPCS system, H-P-C-I. It has its own dedicated DC system, its own dedicated service water system, its own dedicated set of controls, so it is really a third division all by itself. And you will see the effect that has in just a moment.

MR. EBERSOLE: That system doesn't remove heat from the plant, per se, at all. It just dumps it into the suppression pool.

MR. KOLACZKOWSKI: That's true.

MR. EBERSOLE: Why did it make a difference?

MR. KOLACZKOWSKI: First of all, you will see that the probability of it and RCIC failing are considerably less than the probability of the two steam driven systems failing.

MR. EBERSOLE: But the containment failure remains the same.

MR. KOLACZKOWSKI: That is true, but the containment failure does not become an important item until way out around -- the best estimates are now like about 40 hours, that kind of thing. We think that by that time the probability of recovering power -- of not recovering power is just so long that probabilistically speaking, that ends up not being a very important sequence, that in fact you are still more likely to melt the core first due to the HPCS not being available and RCIC also not being available.

MR. EBERSOLE: Where is the battery power coming from in all this time? Are you going to tell us?

MR. KOLACZKOWSKI: The HPCS system, because it has its own dedicated source of power, as long as its battery is running -- excuse me. As long as its diesel is running, it is also charging its own battery. Therefore, the battery power for that division is remaining. You have all control. You have the diesel operating the pump, and that thing just continues to hump along.

MR. EBERSOLE: How do you know what is happening? Where is the instrumentation?

MR. KOLACZKOWSKI: There is instrumentation on that third division so that you know the status of the plant and the status of the system. This outlines the basics of the base design on the HPCI and RCIC systems. I won't go through that in detail.

(Slide.)

MR. KOLACZKOWSKI: There are two sequences here that become important with regard to station blackout. Again, the U1B1 has to do with initial unavailability of the HPCI AND RCIC systems to respond to the accident. Those are the only DC-dependent decay heat removal systems you have. So if those do not respond and you do not recover power in sufficient time, then you will undergo core damage.

Then the U2B2 sequence has to do with HPCI and RCIC initially working but then failing later due to really a variety of failure modes ranging from battery depletion effects to loss of ventilation effects to possibly getting water in the steam drum due to shutting on and off of these pumps and then the water getting into the turbine, that kind of thing. There are a number of things that play a role there.

(Slide.)

MR. KOLACZKOWSKI: Therefore again for the two sequences you see the mean probabilities for again a simple two division type system. The first sequence is driven by the unavailability of HPCI RCIC, and then the second sequence, the more dominant one, having to do with DC and ventilation loss effects on the continued operation of HPCI and RCIC and whether or not the operator can go down and respond.

This is the one I was talking about where, by the time this happens, the operator has to go down into a room that is 150, 170 degrees, and he wouldn't want to be there for so long, so we didn't want to give a very high chance of operator success here.

(Slide.)

MR. KOLACZKOWSKI: Similarly, you can do

sensitivity such as -- what about if the operator cannot or could with some better chance be able to run HPCI and RCIC without ventilation. Again, within the sensitivity bounds we have investigated here, it doesn't have a significant change in the overall core damage probability. Again, the blackout probability way down at the bottom, of course, is the major thing again where you can get a considerable reduction in the core damage frequency.

(Slide.)

MR. KOLACZKOWSKI: Lastly, remember I mentioned we took the newer BWR's and broke them into two groups, this being now the HPCS design, the BWR 6. The important factor here is that HPCS has its own dedicated DGDC service water controls, instrumentation, et cetera. Before we saw 10^{-5}. Now you are seeing more like 10^{-6}.

Again, the same two sequences are the important ones, but now from a relative standpoint the core damage frequencies are like a factor of ten less than the other designs.

(Slide.)

MR. KOLACZKOWSKI: There are the mean probabilities, again, the factors that affect the sequences.

MR. EBERSOLE: These plants that you were just describing still have the same sorts of diesels with the same sort of fuel, the same sort of general design configuration for the diesel plants. You are evidently telling me that it is the dependency in the electric context that gives the advantage in the electric distribution context.

MR. KOLACZKOWSKI: Yes, the fact that you have a third diesel, typically smaller, usually less susceptible to failures, dedicated to just that one pump, and some other controls and instrumentation associated with it.

MR. EBERSOLE: They still have the same diesel mechanics, same kind of oil.

MR. KOLACZKOWSKI: Oh, yes, and there are still potential common modes between the third diesel and the rest of the plant. That's been factored in.

But the third alternate system, if you will, with its own power and service water and so on, does significantly decrease the core damage frequency here.

MR. DAVIS: Excuse me. Without AC power, you can't cool the suppression pool water. It was my understanding that the RCIC will trip on high steam exhaust pressure as the suppression pool water becomes warmer. I don't see that on your table of events. Is that a longer time?

MR. KOLACZKOWSKI: Yes. That is also another reason why the RCIC, or in the previous design the HPCIs and the RCICs, might fail later. That turned out to be not so dominant because it is way down the line. It is not as dominant as the DC failing at five hours into the accident or the fact that you have lost ventilation in the pump room; that those dominate way before you get to those problems of the exhaust pressure and the high temperature, based on SASA analysis.

(Slide.)

MR. KOLACZOWSKI: One thing that was not addressed in the current version of the report very well, and which we have gone back and taken a better look at, is station blackout and a loss of instrumentation.

As pointed out by Mr. Epler, it is important to know what the plant status is. You are relying on just DC backed vital instrumentation to tell you what the status of the plant is. Without that instrumentation, the operators are virtually flying blind.

We looked at various inverted designs, at vital AC configurations for instrumentation, and we did find one design that is probably the most susceptible.

Basically that design is configured such that you are again looking at a simple two-division AC/DC system. You have two inverters for vital instrumentation where you are supplying power. If you should lose AC, you are supplying power from the batter buses through inverters, and eventually into your instrumentation. AC is the preferred source. That is the source they are normally being powered off of is coming off of an AC bus, off the MCCs, and that there is a mechanical switch. It is not a solid state switch. It is physically a relay or a contact that must change place so that when this preferred source of power AC is lost, as it would be in blackout, the switchover must take place so that it switches over to the battery source so the instrumentation can continue to operate. This design is probably most susceptible, and based on the data we have on inverter reliability, switching reliabilities and so on, it looks like the frequency of this occurrence for this design, and again, a simple two-division AC/DC system would be like on the order of 10^{-5} per reactor year. We don't think the core damage probability is all that high, primarily because if the operator -- first of all, he will know that he is in a station blackout. If he has also lost instrumentation, we feel that among other things, like trying to get power restored, one of the things he is definitely going to do is go down and find out why he doesn't have this instrumentation. I would think with the known history on inverters and switchover capability and so on, that's one of the areas he would definitely have checked out right at the beginning, and typically what happens is that this switchover does not take place. It is something that you can easily recover from. You can switch that over. You can get your instrumentation back and provided you don't have any other system failures, the core damage probability is probably very low because of the loss of instrumentation. Again, it is a factor we want to point out. It is something we need to review and review in a specific plant to make sure you are not susceptible to this kind of event.

(Slide.)

MR. KOLACZOWSKI: Comparison of the base design, simple division, base case analysis with safety goal, you see the four basic designs, the total core damage probability, and those are some of the mean values. We pointed out the possible range on external events. You see that compared with the proposed core melt safety goal currently being looked at by the NRC. I should point out again that this is only for the base design, that many designs will have less susceptibility to station blackout, they will have better reliability in their auxiliary feedwater trains, whatever, and so for many plants this comparison will be much more favorable ni terms of comparing to the safety goal.

(Slide.)

MR. KOLACZOWSKI: A word about containment failure. Basically we looked at six different containment designs currently in use in the industry. The ice condenser, small and large drive Mark 2, Mark 1 and the Mark 3. What I am saying here, depending on the containment design used, indeed, the time you have before potential containment failure can vary considerably, and the containment failure modes can also differ, although for the most part overpressure continues to play a dominant role in all the containment designs although again the time you have before that overpressure event can change considerably.

One thing I want to point out about the ice condensers in the Mark 3s, you will notice it says at or after AC recovery. One of the things currently going into the ice condensers of the Mark 3 is the use of igniters. That's fine given you can burn the hydrogen as it is being generated, or perhaps it is fine. However, in a station blackout event, all the igniter systems that we have looked at rely on AC power to operate. Therefore they will not be able to burn the hydrogen as it is generated, and given you have suffered core damage and generated a considerable amount of hydrogen in the containment, then should you recover AC power, it is designed such that thge igniters will come on automatically or by procedure, the operators turn on an igniter, he will turn it on in an environment that is very hydrogen-rich and bad things could happen.

So here is a partaiculr set of sequences. And turning them on is detrimental rathern than helpful It brings out the importance of once AC is restored, knowing what systems you want to bring on line and in what order.

MR. PAULITZ: I've got a question. Before you taked that slide off, would you explain the eletrical penetration failure on the Mark 1 and 2 for a little bit?

MR. KOLACZKOWSKI: Apparently on the 1s and 2s, there are some designs that the electrical penetrations that are on the drywell are not indeed welded penetrations, but they use an organic type seal, and the SASA identified a failure mode whereby the increasing temperatures in the containment which will occur because you have lost drywell and so on, will degrade the seals, the penetration will rupture, and it will blow out way before, not way before, but a number of hours before you would suffer a potentoal overpressure to the containment.

So indeed you end up with a bypass path for radioactive fission products to escape through this penetration and out into the environment.

(Slide.)

MR. KOLACZOWSKI: In summary, as far as the things that appear to be important to the station blackout issue, here is a list from a sort of generic perspective. That is the standby reliability of decay heat removal systems is certainly important. DC reliability and battery capacity, trying to extend that, and including instrumentation and control is a vital issue and something that needs to be looked at on a plant by plant basis.

The common service water dependencies we have discussed. The loss of reactor coolant system integrity is important to some plant designs; trying to show the effect of different containment sizes and design pressure on the timing and therefore the potential risk from such an accident. Operator training and procedures are important. I will discuss three important factors in a moment, and then external events.

(Slide.)

MR. KOLACZOWSKI: On a major plant type basis, PWRs, again we have to look particularly at the auxiliary feedwater system unavailability, battery depletion effects on continued operation of the auxiliary feedwater system; and again because you suffer in not having reactor coolant system makeup capability under loss of AC conditions, if you fail RCS integrity that is an important item.

The BWRs, again the RCS integrity loss is important. HPCI and RCIC, it is the case of being able to continue to operate those under a prolonged period with loss of ventilation, eventual loss of battery, or power, et cetera. Then the HCSC RCIC designs, these are important factors.

(Slide.)

MR. KOLACZOWSKI: There are three important human actions. The first is obviously to recover AC power. That is a simple statement, but I might say that there are some very important procedural aspects there that need to be considered, things like are you going to send everybody down to one diesel or are you going to try to work on multiple diesels at the same time?

If the blackout is for a prolonged period, do you have procedures in place such that the dispatcher puts you high on the list in terms of places he will recover power to first, whereas versus if you are running on your diesels and everything is fine, maybe hospitals and medical facilities are more important to get power to them first rather than to the power plant.

Extending battery life, I think we have gone into the fact that DC battery depletion has a significant effect on many of the designs, and anything he can do to strip unnecessary loads and extend that batter life is certainly important.

MR. EBERSOLE: May I ask a question at this point? I have been seeing that the diesel engines have an interesting source of air supply. They are normally pumped up by AC driven compressors for the air supply, but at the bottom line, most of these diesel plants have an engine driven small diesel air compressor which gives them sort of a black start capability. They can start their own diesel with which to start the big diesels using small engines.

Well, to lift that sort of concept into the battery area, is it possible that what we really might consider is an engine driven DC power supply for the rare but admitted case of loss of DC power? There is not much investment in it.

MR. KOLACZKOWSKI: That could certainly be a possibility, something we could look at for future designs. I think you have to separate that from backfitting and you need to look at whether that is really a necessary thing to do, if it is really an advantageous thing to do in a backfitting situation, or are there other aspects of the plant design or operation which would essentially counteract that so that blackout is maybe not important to that plant, and maybe that kind of a fix is really not necessary. I think you have to look at it on a case by case basis.

MR. RAY: I should think that any station superintendent that was worth his salt, if he saw that he was in a situation where his battery was going to determine his life or death, he would jerry-rig something by bringing in a motor-driven auxiliary jack.

MR. KOLACZKOWSKI: Yes, and I think that given enough time I think that is something he could definitely do. In the meantime, I think he ought to do and have procedures in place to recognize: What are my unnecessary loads? Which ones can I strip? When can I strip them? So that that is laid out so that the operator isn't right then in the situation trying to guess what he can strip and what he can do; that he has procedures in place to tell him how to extend his battery life. And we have talked about the last item about it being important as to which system he is going to bring back on and in what order.

(Slide.)

MR. KOLACZOWSKI: Okay. What I hope I have done this morning is that in trying to address how important is station blackout in looking at the accident sequences and potential core damage probability and risk; that unfortunately no one answer exists. We have not found a single widget that if you added that everybody's problems would go away; that it does depend on different plant features and operations. However, we feel that the base case analyses we have done and using with those concurrently the sensitivity analyses in the study, we can actually cover a variety of plant designs and even investigate specific plants on a plant by plant basis.

With that, I guess that concludes my remarks unless there are other questions.

MR. RAY: Allen, what is the status of your report? Is it in final form now? Has it reached the point where your revisions have been determined and you are producing it?

MR. KOLACZKOWSKI: As Pat pointed out, we are on a schedule to try to get it out by October. NRC has been reviewing it, and a number of branches within the NRC have been reviewing the report. You people also had the report. We are getting comments back to us now and incorporating those. Essentially we are working on the final revision currently and do plan to have it out by October.

MR. RAY: Has a copy of this been distributed?

MR. SAVIO: Yes, sir. It was about three weeks ago.

MR. RAY: It is availale to us.

Is it available to industry?

MR. KOLACZKOWSKI: Pat, I guess you'd have to answer that question.

MR. BARANOWSKY: No.

MR. RAY: Will it be?

MR. BARANOWSKY: It will be available as soon as it is published. What you see here is some draft material that we have made available for internal review. I don't normally publish interim results for industry review. On the other hand --

MR. RAY: I wasn't thinking in its present state. It will be a NUREG or something?

MR. BARANOWSKI: This will be a NUREG contractor report, and hopefully it will be available in October. Now, at that time I would hope industry would take a look at it, and given that there are some flaws or problems with it, let us know so that when we go through that next year of formulating positions and so forth, we can make appropriate corrections. I don't think there are major flaws in the work, but I think that's the kind of review we would like. The thing should be published as a NUREG.

MR. RAY: I would think industry would be most anxious to get a copy of this so they can do some self-analysis and determine what their prospects were for major changes on the plants down the road.

MR. BARANOWSKY: I think one of the things worth doing is taking a look at how your plant stacks up with all these different sensitivities that have been done in order to see if it looks like you might have a problem.

MR. RAY: Okay.

Are there any questions for Allen from the panel?

(No response.)

MR. RAY: Okay, we will take a ten minute break and return for the Oak Ridge Report.

(A brief recess was taken.)

MR. RAY: We will resume the meeting.

At this time we will hear from the Oak Ridge National Laboratory Team on the work they have done on reliability of emergency AC power.

(Slide.)

MR. BATTLE: My name is Ron Battle. I work at Oak Ridge National Laboratory, a d I will present the results of our analysis of emergency AC power systems for nuclear power.

(Slide.)

MR. BATTLE: The purpose of our study is to provide a technical basis for the NRC to resolve station blackout, the generic issue of station blackout. We did this by estimating reliability of AC power systems. We identified factors important to reliability, and we estimated some costs of some of the improvements.

(Slide.)

MR. BATTLE: The scope of this project is to offsite power analysis and onsite power analysis. I will summarize some results of offsite power and present -- most of my presentation will be in the onsite power.

The onsite power, ask you can see, is design review, looking at a lot of operational data and reliability analysis.

(Slide.)

MR. BATTLE: The loss of offsite power, we looked at frequency of events and restoration by cause, and we looked at important design and operational factors that affect offsite power.

(Slide.)

MR. BATTLE: Here I have a curve that shows -- broken down by system or by plant cetered an areawide factors, to show frequency versus duration of loss of offsite power.

As you can see, the most frequent events are plant centered, and it tapers off -- it probably reaches zero somewhere between 10 and 100 hours. It would have to be quite a serious event to go more than 40 hours or so.

(Slide.)

MR. BATTLE: Some of the factors affecting offsite power availability in the design are interconnections of the switchyards. We have identified this. Normally they receive their preferred power from one source, the switch yard. There are normally two sources, and you also have to transmit power, of course. Frequently the switch yards are connected together, and they frequently go down together.

Some plants have a separate line that is not normally connected to the switch yard, and it seems to survive.

MR. EBERSOLE: I wonder if you would go back to that curve a moment where you showed the generic frequency and duration. You show something like a one hour power outage oh, once every five or six years, all causes combined.

Could you give me a comment on the spread of data?

Is that a national average? What's the worst utility that I've got because I think this is the kind of information that misleads you because of its median aspects. We may have a half a dozen utilities who are the only ones we really need to worry about.

MR. BATTLE: In our report we do break it down into some utilities --

MR. EBERSOLE: Where is the worst one like that?

MR. BATTLE: .25 is like an average for some of the worst plants.

MR. EBERSOLE: For how long an average?

MR. BATTLE: I don't remember restoration times. Florida, you could look at those as an example. They have St. Lucie and Turkey Point, and they have quite a high frequency.

MR. EBERSOLE: That's the one I was thinking about by the way.

MR. BATTLE: They say they can repair theirs like on an average of 30 minutes.

MR. EBERSOLE: Simply on a reporting basis, don't you think it is important that you show the lower end of the spectrum when you show a curve like this? This is really deceiving to the average reader who reads that and says hmm, that's pretty good. What it doesn't show is we have got a substantial number of plants that are in big trouble.

MR. BARANOWSKY: The factors we are talking about in terms of the upper end of the spectrum are factors of like two to three. We are talking about uncertainties in the whole station blackout issue of 10 to 20 or 30. The Sandia guys have cranked these uncertainty factors in the analyses. This curve is not misleading in that it presents average data. It would be misleading for us to present an upper bound and say here is what all plants look like. We recognize that some plants are more prone to losses of offsite power and of significant durations, and for that reason, you may recall that I said we would like to see some minimum requirements plus possible tradeoffs. That is to say the plants with the less reliable offsite power circuits might be required to have more reliable onsite power circuits. So this factor would be taken into account in any regulatory position that would evolve. And when we do finish the offsite power reliability report, I think you will see considerations in there for plants that are on the upper end of the spectrum, and we will try to address them appropriately.

MR. EBERSOLE: The worst case is only a factor of two or three away from the average?

MR. BARANOWSKY: (Nods in the affirmative.)

MR. EBERSOLE: And we are dealing with what, factors of 20 or 30?

MR. BARANOWSKY: In terms of overall uncertainty. Now, the factors of two or three relate principally to losses of up to about one hour. As you get into losses of like ten or twelve hours, the distributon spreads. You are talking about probabilities. There are frequencies, let's say, of .01 to .05, as an average, and there is a chance at that point that a factor of two or three could be a factor of three to five or three to six, something like that. I have seen published some places analyses that show that offsite power losses of like eight to ten hours or something along that length of time are like 10^{-3} or even less, and that is even hard to believe.

MR. EBERSOLE: Is this related to hurricane damage?

MR. BARANOWSKY: No. Using Baysian analysis to correlate data from several sources. I personally have a problem with that because I don't think we know that the once in a thousand year frequency in terms of duration of outage -- well, we just don't have the data base for it.

MR. EBERSOLE: I guess one of the things that bothers me, what you say implies so if the worst end of the spectrum is only two or three worse than the average, you really -- we have a number of extremely strong grid designs. You say there is a point of almost no return in that region because the problems are inside the plant.

MR. BARANOWSKY: I am not quite sure I understand.

MR. EBERSOLE: We have some very strong and very weak offsite power systems.

MR. BARANOWSKY: Oh, yes.

MR. EBERSOLE: You are telling me it doesn't make any difference.

MR. BARANOWSKY: It doesn't make a world of difference, okay, but factors of two and three. It is not factors of 10 and 20.

MR. EBERSOLE: Right. Thank you.

(Slide.)

MR. BATTLE: Another design feature that we looked at is alternate power sources near the plant such as a gas turbine or a coal plant. In operation there is restoration procedures, both at the plant and by the dispatcher that have to be considered to restore power. We are looking a little further into restoration time. Geographically, factors affecting reliability are grid stability and weather. We are looking a little further into some correlations with weather and reliability of onsite power.

MR. EBERSOLE: Did you look at the Savannah River and Hanford designs and notice the striking difference in their approach to power system reliability, the difference between that and commercial reactors?

MR. BATTLE: No.

MR. EBERSOLE: You didn't look at the production plants. Well, there is a complately different philosophy they use.

Okay, you didn't look at it. Okay.

(Slide.)

MR. BATTLE: The onsite power system reliability consists of a design review, operating experience review, and reliability analysis. The remainder of my presentation willk be on this system.

(Slide.)

MR. BATTLE: First, I'll discuss some of the limitations of this analysis, the boundaries that we have put on that. We looked at SARs for most of our data. We did get additional data from plant visits and other questionnaires and such that are available in some detail. We reviewed procedures from a number of plants. We looked at some other PRAs to see what insights they might give us into how we want to conduct our study. We used operating experience to guide us in that also. We tried to limit our study, not to be a plant specific study in that we don't want to get down into the details that are unique in one particular plant, but we want to use enough information that we have representative information. It is not just the generic design, but it is no so detailed that it is unique to that plant and only useful to that plant.

We have already discussed that LOCA was not one of the events we considered, and based on this, that determined the number of diesel generators that we would require in providing AC power to the system.

We stopped where the accident sequence study took up, where Allen's study carried on.

MR. RAY: You say LOCAs were not included, but I see there you included small LOCAs.

MR. BATTLE: That's right. That's essentially the difference in the fast start of the diesels and the number of diesels that would be required.

MR. RAY: But you really excluded, I gather, then, the large LOCA rather than all LOCAs.

MR. BATTLE: Yes.

MR. RAY: On your second bullet, past operating experience, what was the source of the information on past operating experience?

MR. BATTLE: I have a slide on those sources.

MR. RAY: Thank you.

MR. BATTLE: Interactions that are important to the diesels are -- one is the cooling system. Some plants are cooled by some -- some diesels are cooled by service water and some are air cooled. The diesels cooled by water are dependent on the plant service water system, DC power. Some plants have dedicated diesel batteries and some depend on plant 1A batteries strictly. We found that even those with dedicated batteries, they are also dependent on the plant 1E battery to supply AC power to the system.

Offsite power, there are interactions through the control system, relay logic and whatnot that can make onsite and offsite dependent on each other. The NRC has looked at the problem of low voltages such as occurred at Millstone in '76. They have treated this problem for a number of years now, so we did not include these events, this event, in our analysis.

The paralleling of power sources is another possible interaction. This is normally interlocked so that you can't parallel them. We assume that these interlocks function to prevent your paralleling the power sources.

(Slide.)

MR. BATTLE: When we started our analysis, as I said, we did a design review. We took the SARs and ot her sources of design information, and we looked, starting at the switch yard, and we went all the way down through the diesel and looking at its subsystems and their dependencies. We looked for common cause failure modes in the design where we could see them, and we looked at their interfaces with other systems in design. We collected procedures where they were available, and during othe course of the analysis, we did some site visits, discussed operating procedures, designs. We observed some tests to see how they followed their procedures, just to get a general feel for how the design and operation interacted.

(Slide.)

MR. BATTLE: We looked at the configuration of the diesels for all of the plants that are now operating. We selected from them 18 plants. We selected ones that were representative of what is out there as far as their configuration. The 1 of 2 here would mean two diesels available, but they would provide one to provide shutdown AC power. We selected 11 of those plants. That's the most common configuration in the industry right now. And then we selected several plants from these other configurations.

MR. EBERSOLE: In that configuration column, is there any difference between the case where you have a coincident large coolant -- you are not --

MR. DAVIS: What about shared and swing diesels? How do you pick those up in your configuration?

MR. BATTLE: Well, like the 2 of 3 unit, we woulk say -- that would be for a two unit plant that yas three diesels. So it would require two diesels. One of them would be a swing diesel.

MR. DAVIS: I'm thinking of the Surrey configuration where each plant has two and then there is a swing diesel.

MR. BATTLE: At Surrey each one has one. That would be 2 of 3.

MR. RAY: Do I interpret correctly from something you said on this slide at the outset that the number of plants selected with these specific characteristics reflects the population of plants in the industry?

MR. BATTLE: We didn't select them based only on that. We looked at the diesel manufacturer, the age and configuration of the plant. In some cases we selected some to get some of the different NSSS vendors. So we tried to be representative of many different factors.

MR. RAY: Not just the population of 1 of 2 and so on?

MR. BATTLE: That's right.

MR. EBERSOLE: The 1 out of 3 plant, which one is that?

MR. BATTLE: Yankee Rowe.

MR. EBERSOLE: Yankee Rowe, old timer. And the 2 of 5?

MR. BATTLE: That woulds be Hatch and Farley, and I guess Zion.

MR. PAULITZ: That Yankee Rowe was retrofitted a number of years ago. They had none. They did have a hydro facility up the road. That was before the Northeast blackout.

MR. RAY: You mean it was retrofitted before that?

MR. PAULITZ: After.

San Onofre started out with none. Then the Northeast blackout came along and they got diesels.

MR. BATTLE: There were a couple of designs we didn't model. That was 1 of 1, Big Rock Point, and Brown's Ferry has eight diesels. We didn't model that.

(Slide.)

MR. BATTLE: Looking at saome of the operating experience data, we loo at the data sources, we did a statistical analysis and we did a common cause failure analysis.

(Slide.)

MR. BATTLE: Our best data came from the station blackout questionnaire which we sent out to the utilities. We got data from about 36 plants and about 90 diesels, consisted of the number of failures, the demands, the test and maintenance unavailability, repair time, ane we also got some data on modifications. We also got some operational experience data from NUREG-0737, which is the ECCS questionnaire containing many other things other than diesels. But there were 22 plants and 58 diesels in that. Most of it had outage data and repair time or down time. And of course, we used the LERs.

MR. PAULITZ: I'm glad somebody is using

them.

(General laughter.)

(Slide.)

MR. BATTLE: I'll present some of our statistical results and compare them with the reent EPRI study. We calculated failure on demand. We have an average of about 2×10^{-2}. EPRI was 2.3×10^{-2}. The ranges are close also.

By the way, we have quite a bit more data than they do, so some of these factors might change, and their results might change a little if they had some data. Failure to run was 2.4×10^{-3} average for us, and we calculated this for all plants, not only on a plant specific basis.

MR. RAY: Explain for me the difference between those two categories.

MR. BATTLE: Failure on demand is failure of the diesel to start. You ask it to start and it doesn't.

Failure to run was the diesel does start, but then it fails sometime later.

Ours was 2.4×10^{-3}. At EPRI they calculated for two plants, 1.4×10^{-3} to 1.5×10^{-2}.

MR. EBERSOLE: Pardon me. Run how long?

MR. BATTLE: We based our data on -- well, this is failure per hour. I didn't put that on there. I'm sorry. This is the failure rate.

MR. EBERSOLE: Failure per hour.

MR. BATTLE: We looked at unavailability of the diesel and how much that would contribute to system unreliability. I'm putting these numbers up here to compare them to EPRI, but the average we used here was lower than that because we only considered the down time while the reactor was operating, and the average for that was 4×10^{-3} but we did use averags.

MR. KASTURI: Did you include the second run category? These are starts and loading sequence. That is failure to start?

MR. BATTLE: That's right.

The average unavailability compares pretty close. The hour range was much greater than theirs. I think it is because of the difference in the data, the amount of data. The mean time to repair at the EPRI study did some testing. Our mean time was 32 hours.

MR. RAY: I wasn't listening hard enough.

On Item 3, T&M, what does that mean?

MR. BATTLE: Test and maintenance, scheduled maintenance, reactor down.

MR. DAVIS: On that issue, do you assume that even if the unit is experiencing test and maintenance then they demand, that you automatically assume it fails, even though you may be able to bring it into service in time to restore AC power?

MR. BATTLE: No. We don't give it -- well, I guess you could apply the repair time to it. A lot of the test and maintenance would be an overhaul of the diesel. It is completely torn down, and really, you couldn't return it to service very quickly from that service.

MR. DAVIS: It is possible for a diesel to be overhauled while a plant is operating? I thought there was a tech spec limit.

MR. BATTLE: There is 72 hours on the number of plants.

MR. DAVIS: The answer is you didn't give any credit for test and maintenance, is that right?

MR. CAMPBELL: I would like to respond to that.

I'm Dave Campbell with JVF Associates.

One thing we did observe at all of the plants we visited -- and I assume it is the case everywhere, is thre is no real contribution here from testing the diesel because every plant does have a test override capability. so what we are really talking about there is scheduled maintenance and -- well, the number we used was scheduled maintenance during the time the reactor is operating and does include some time the reactor is shut down as well.

MR. BARANOWSKY: Let me also add one thing on that 72 hour tech spec limitation.

There are some plants that have a seven day tech spec outage limit for diesel generators, and whenever a utility has, let us say, a lesser allowed time in their technical specifications and finds the diesel is going to be unavailable for a period longer than their tech spec will allow, they will come in to the NRC and ask for a exemption or an emergency tech spec change, a one time type of thing. So they may for some reason or other find out that the diesel is in an inoperable status, that they have to tear it down, and they are not going to wait for a refueling to do that. They are going to try to get it done with an emergency tech spech change. That will be discussed a little bit this afternoon also.

MR. BATTLE: For a common cause failure, I show ranges for the two studies. I don't show here categories. We looked at human failures and hardware failures, and EPRI also has not a category. Ours is from 1×10^{-4} to 4.2×10^{-3}. These are probabilities. EPRI's is 1.7×10^{-3} to 8.4×10^{-3}.

MR. DAVIS: What are those numbers exactly? Is that the probability that you will lose all diesels?

MR. BATTLE: That is the probability that you will lose sufficient AC power, for example, if you have to have two out of three diesels to cool your plant, you have to lose two diesels. That is the probability that you would lose those two, at least two diesels.

One thing here is EPRI took plant specific data and did a Baysian analysis. We took all the data from the industry and applied the data as it would fit to each plant in their specific design, how their category would fit to that design.

MR. KASTURI: Did you explain common cause as saying you would lose a sufficient number of diesels? Does that mean you would have considered factors beyond common cause in these failures, because I could have put one of these on a test or maintenance and the other one might not start. Would that be in your category of common cause?

MR. BATTLE: No, that would have been common cause. We do have the probabiity that the diesel will be unavailable for test and maintenance. That will contribute to the unreliability of AC power, but it is not common cause.

MR. KASTURI: You truly looked at the commonality of why diesels did not start? Is that how you looked at it?

MR. BATTLE: That's right.

For the demand data, we have an average of about 32 demands per year. This is averaged over all the plants. The range is from 12 to 85. By the way, for most plants this is considerably more than would be required for their testing. EPRI has an average of 36. It ranges from 36 to 80. So there are quite a few more demands than you would anticipate a plant to have, just looking at their scheduled testing.

MR. KASTURI: This does include the testing, though?

MR. BATTLE: Yes. As a matter of fact, one of the differences in our data might be that we took out some of the tests that were done for maintenance. If the diesel failed and they kept repeatedly testing it while they were in the process of repairing it, we didn't count those as what I would call a valid demand. We were looking at demands where they were testing to see if the diesel would function under an emergency condition.

MR. RAY: Do you have any idea as a result of your work as to why there are so many demands as compared with the requirements for testing?

MR. BATTLE: We do have these demands broken down by type, and they vary. Some plants test, do regularly scheduled tests more frequently than is required. In addition, they have LCO tests. There are some actual demands by loss of voltage on a bus or inadvertent safety injection system. There were a couple of categories, and they all added up to make it much more than their scheduled tests.

MR. BEARD: J.T. Beard. We are going to be discussing that this afternoon. I guess the bottom line, not to pre-empt anything, but basically the number of test starts breaks down from the scheduled maintenance which could be once a month or scheduled testing once a month, and that stacks up, it could be as frequently as once every three days you are required to test all the diesels. The other major contributor is, when they have a diesel down, they go into an action statement in their tech specs which requires for the newer plants that all diesels be started on an every eight hour basis. If you are into that sort of a position, every eight hours begins to rack up a lot of starts, but we will be discussing that this afternoon.

MR. RAY: But those are required starts. The point was made that the actual experience significantly exceeds the requirement.

MR. BEARD: I don't want to speak for Mr. Battle, but I think what he said was that the testing requirements under a routine situation where you do not think there is anything wrong with the diesels, but you are more or less testing it on some frequency to show that you have the reliability you think you do, that might be, say, once a month. Now, once a month comes out to 12 a year. The reasons these numbers are higher than 12 a year is for more than those situations. You are right, the other tests are required in most of the cases by the NRC.

MR. EBERSOLE: The second and third and fifth lines, that is all per generator per demand, right?

MR. BATTLE: This would be failure per hour (indicating).

MR. EBERSOLE: Per generator.

MR. BATTLE: The others are probabilities there will be failure on demand.

MR. EBERSOLE: So when you get the whole set there, it looks like you may be getting 96 percent that failed to do their thing? Right? Ninety-six percent for reliability is an approximation.

MR. DAVIS: Per diesel?

MR. EBERSOLE: That is all per diesel, isn't it?

MR. CAMPBELL: I would like to add one thing to that on the test and maintenance unavailability. You don't have that contribution from two different diesels at the same time, so you really can't add that together and multiply those to get the system reliability.

MR. DAVIS: The question on the failure to run number again, it would seem to me that that number varies considerably to run. That is, the first hour you would expect a much higher failure probability, I think, than you would after several hours. Is it permissible if you need the diesel ten hour to multiply that number by ten and that gives you the failure probability for a ten-hour period?

MR. BATTLE: We didn't assume that the rate changed. We assumed that this was a constant from after it started until we didn't need it any longer.

MR. DAVIS: In your data base, how long did they actually run them to get that time?

MR. BATTLE: That failure to run data we got from failure to run all of the starts, all of the tests that were scheduled to go more than six hours, and we took the number of failures from those and calculated the failure to run from that data.

MR. EBERSOLE: Did you find out why the failure to run, why there were failures to run? I have understood this is to a great extent oriented toward the time and heat degradation as such things as emerging seals and rubber hoses, that they get old.

MR. BATTLE: That was some of them. They got some rupture in some of the service water hoses and sprayed the diesels.

MR. EBERSOLE: This would actually make the failure to run rise with time rather than fall.

(Slide.)

MR. BATTLE: Here I plotted the distribution of our failure on demand, just to show you that it does vary considerably, nearly an order of magnitude.

MR. EBERSOLE: Now, I am trying to digest what that means. That means you have some very bad ones?

MR. BATTLE: Yes, some have much higher failure probabilities than others.

MR. EBERSOLE: Could I identify a group of those and say, these are really the ones that need the attention?

MR. BATTLE: We have identified the ones that have high diesel failure rates, and then we have also shown where that was important, for which plants that was a factor.

MR. EBERSOLE: I see. We are coming to that. Thank you.

(Slide.)

MR. BATTLE: We did an analysis by subsystem to see if there was one fix you could do to improve independent diesel reliability, and there is not. They are all spread fairly evenly. You could spend a lot of money fixing one subsystem but you are still going to get something else to cause a failure.

MR. EBERSOLE: Do I understand that the start systems were almost universally better if they used compression air rather than the little starting motors?

MR. BATTLE: Well, I can't say that is so.

There is some speculation that direct injection into the cylinders might be better, but they have had distributor failures. They fail also. A big problem in the air start system is moisture that has been identified by many people. Air motors fail because of motors but also the valves and systems fail from moisture, too.

MR. BARANOWSKY: Ron, before you go on, I was wondering if you might identify how specific plants don't find these averages holding through whereas they may have a chronic problem due to one cause.

MR. BATTLE: Yes, that is a good point. This is over the whole industry. Now, a few plants will have a high probability from one system. I always like to point out Farley, prior to 1978, they didn't have air driers in their air start system. They installed it late in '78. Prior to that they had -- I have forgotten the number of failures. Quite a few. Six or seven, on that order.

MR. EBERSOLE: Air driers are loaded with dessicate, isn't it?

MR. BATTLE: There were some that used dessicants and they blocked the system, so now most of them are installing refrigerant type chillers, but since they have installed it, they haven't had a single air start failure. I have been looking over the past year or two to see if they have had some since we quit the analysis, and they haven't had any that I can find. It seems to be working pretty well for them.

The point is, each plant is going to have to identify, if they have a problem, and they are going to have to fix it.

(Slide.)

MR. BATTLE: We have broken common cause down into two categories, human error contribution to common cause, and next I will discuss hardware contribution to common cause. First I will show, we took the LER's, the failures, and we looked for common cause potential or actual common cause, and this is the way the failures broke down into one actual failure, seven weren't available, and there were 51 that we identified to be potential common cause.

We used the EG&G data or method. They have a BFR computer code, and based on diesel configuration and design, we came up with the probability for each plant that we were studying. Here, these are the ranges presented on the slide for the probability of human error common cause. We didn't assume that all human errors were common cause. We looked for the ones that would be, we felt, common cause contributors.

MR. RAY: Ron, I am having trouble with the last column. What do you mean by potential? Were the facts not clear that it was attributable to human error, or it is a matter of interpretation?

MR. BATTLE: By potential, of course, most of the time it is just one testing of a diesel. Now, maybe if they had tested the other diesel, it would have failed also, or at least that type of failure would -- both diesels are susceptible to that type of failure, and although both didn't fail, we considered that as being a shock to the system that could have caused both diesels to fail in an actual emergency.

MR. RAY: Was the second unit in the case of two units actually exposed to the condition that caused the failure of the first?

MR. BATTLE: Well, for example, the problem would be leaving a fuel valve closed. It might be because of a procedural problem. If you left it closed on one diesel, you very likely could have done the same thing on the second diesel.

MR. RAY: But you get charged with that only in the event the procedure was why it was left closed.

MR. BATTLE: That's right, and we think procedure is a big --

MR. RAY: That is the kind of thing you mean.

MR. BATTLE: Right.

MR. EBERSOLE: Ron, let me ask you a question. Have you ever looked at the potential of a diesel engine to have governor failure and to lock the fuel valves wide open without a connected load and seen what the dissenic grading capability is? My understanding is that Lloyd's of London have records of ships being sunk by pieces of diesel engine. Do you all look at the interaction between the diesels?

MR. BATTLE: Most of this is based on experience.

MR. EBERSOLE: I haven't heard of anything like this here.

MR. BATTLE: We don't have such a failure.

MR. EBERSOLE: Is it mechanically possible?

MR. BATTLE: I would suppose it would be. The fuel rack could get stuck open. I don't see why -- it gets stuck open or closed quite often.

MR. EBERSOLE: Should it be?

MR. BATTLE: I think it is probably the more rare event, is what you are talking about.

MR. EBERSOLE: Right.

MR. BATTLE: And there are other events that will get you.

MR. EBERSOLE: Well, you get down to this question of should I isolate these stall by stall to accommodate an engine explosion, and I have never really heard a good answer to that.

MR. CAMPBELL: I would like to add just a couple of things on that. First of all, that would be covered under our hardware common cause and not under human error, but like Ron said, we didn't see any events like that, so we didn't really have a basis for assuming they are a credible type thing. The diesels are isolated. I don't know how missile-proof the walls between the diesel generators are, but they are isolated, and I think the kind of thing you are talking about, just the initiating event, is of relatively low frequency, and then to generate a missile that actually takes out the other diesel generator again is a rare event, so I think probabilistically it is not going to be a main contributor.

MR. EBERSOLE: Also in the context of general degradation of the fuel tanks, they are generally unified with respect to the tank. Do you look at the catastrophic aspects of fuel tank explosions, and how that might really involve -- you are looking at the more mundane type failures?

MR. BATTLE: You are talking about the more remote failures that are probably not going to be the ones we are going to have to worry about. We have a lot of failures.

MR. EBERSOLE: Right. We've got enough without these.

MR. BATTLE: Yes.

(General laughter.)

MR. BATTLE: The main thing we have identified in human error in our analysis is that procedure contributes the biggest part of common cause error. I am not going to say that by procedure you can eliminate human error, but the point I want to make is, you might be able to eliminate the common cause failure by human error or reduce it considerably if you have good procedures. We did some fairly detailed procedural reviews, and categorized procedures by quality. We set up our own standards really because there are no standards to go by. We have had some pretty good correlations between procedure -- quality is what I call it -- and probability of human error common cause failure.

I list here some of the factors that we looked at in procedures when we did our categorization.

MR. PAULIZT: I have got a question. There seems to be an item left out of this common cause business that is other systems and interaction. I hate to keep bringing this up. You can have two independent diesel generator rooms, and some people may have made a common drain down to a separator tank because the environmentalist says we are not supposed to throw oil overboard. You could have problems from the outside getting into both, or problems from one diesel generator room and from the other, be it water, oil, or whatever, and unless these -- or fire protection system in their commonality. Unless these things are looked to in their detail, and they are contributors, I think there is a degree of uneasiness, at least on my part, that we are getting everything in there.

Now, true, some of them have not occurred yet, but that doesn't say that they can occur. If we are only looking at the LER's, that is one thing. If we are looking at how the system is designed and how it relates, then we ought to factor it all in there.

MR. BATTLE: I think each plant has to look at these. If they have a common cause failure mode like that, that is something that they need to worry about. We have identified some from experience that are important.

MR. CAMPBELL: Again, I would like to stress what I consider to be the importance of looking at operating experience. We could sit around all day and postulate things that would knock out two generators, but I think you can argue successfully that if we take a look at the amount of operating experience that we have with diesel generators, and we haven't even seen one instance of a single diesel failing because of a backup drain or something like that, then that is not something we need to worry about.

We have seen instances of single diesels failing because the fire protection system was actuated inadvertently. We haven't seen a multiple failure based on that. The point is, I think on a probabilistic basis we have probably got most of the major contributors to common cause failure that you are going to see.

MR. EBERSOLE: May I comment to that? Suppose I have a modest earthquake. I don't mean a big thing. Well within the probabalistic range we are talking about, 10^{-3}, invading foreign to this area, and let's say I have unqualified lines in the diesel generator, so I get off-site power failure. Okay, now, let's go one step further. We don't require seismic fire protection systems, and this plant I am looking at has the unfortunate characteristics of using CO_2 for fire protection which protects the generator by closing each generator in a box and flooding it with CO_2.

The spurious activation of the fire protection systems will automatically close down generator cooling, and I am locked into a non-functional regime which I might or might not get out of before I burn up the generators. The engines run exuberantly, but the generators are burning up because they have no open site of cooling. Do you all look at that? I just have a modest earthquake. All right?

MR. CAMPBELL: Well, again, what you are talking about is a relatively likely event. I think in terms of the station blackout study, you know, you can't really look at the whole scope of an event like that, because the diesel generators will not be the only things in the plant affected. You might be wiping out AC.

MR. EBERSOLE: I didn't wipe out safety. I wiped out non-safety. I wiped out the fire protection because it is spuriously activated, and a loss of off-site power.

MR. CAMPBELL: That can actuate and knock out other safety equipment as well.

MR. EBERSOLE: In a common mode manner.

MR. CAMPBELL: This in my opinion is not just a station blackout issue. I think it is an important consideration.

MR. EBERSOLE: It is a station blackout that is generated by a modest earthquake.

MR. BARANOWSKY: But you could also say what happens if non-safety systems that perform other functions fail? Is that a problem? Well, yes, it's a problem. It's something that one has to be aware of in the design of plants. We showed earlier, at least in the Sandia presentations, that non-seismically qualified equipment must be considered in terms of the hazards associated with an earthquake related to station blackout, but the same thing could be said for any other type of characteristic accident. If the Sandia guys have done more on this and would like to address it, I think they should right now.

MR. KOLACZKOWSKI: Again, as I said before, we did not try to in a detail way go through the actual individual scenarios that might happen given a seismic event, but I think we have identified a seismic event of the magnitude and frequency you are talking about. Yes, it is important, and we have tried to point out the areas that need to be looked at. Beyond that, you are looking at considerable detailed analyses and perhaps even a plant by plant analysis which was well beyond the scope of what we could do here.

MR. EBERSOLE: Is it also beyond your scope to have done this sort of thing?

MR. BATTLE: Well, yes. We can't go into all other systems, either.

MR. EBERSOLE: You can't look for the cotter keys.

MR. BARANOWSKY: It is not beyond my scope. This kind of thing should be addressed in terms of a regulatory position, and it would be. It's an interface item that has to be addressed.

MR. EBERSOLE: Right. Thank you.

(Slide.)

MR. BATTLE: The other cause we looked at was hardware common cause failure. Here we see actual experience, the data we have, and the range of probabilities. The events we found, the design features that cause these hardware common cause failures, are fuel blockage and extreme room temperature, service water blockage, water in the fuel jacket, water corrosion problems, and air start interconnections.

The design features that contribute to common cause failure. Where the designs existed in the plant, we included probability of that particular common cause failure in our specific design analysis.

MR. DAVIS: Did you find any instances where common exhaust ducts were used or common air intake ducts that would lease to a common cause failure procedure, or a common lube oil system?

MR. BATTLE: I didn't see any of those. There may be some out there, but I can't --

MR. DAVIS: I've seen that kind of thing in aux feed systems.

MR. BATTLE: The one kind of system might be the fuel system. I know it is in some cases. They will have one large fuel tank where they put all their diesel fuel in front of that tank. They will supply separate tanks. That is where this water can be entered into that tank (Indicating) or you can have condensation to get in there. If you don't have a way of removing that water, you've got a common cause failure potential.

MR. EBERSOLE: Did you look at common vulnerability to deliberate acts of damage?

MR. BATTLE: No.

(Slide.)

In our reliability analysis these are the factors we looked at. We've already discussed them. Human errors, hardware, common cause failure. We looked at service water, DC, offsite power systems failure. Those were obtained from other sources. We didn't come up with these probabilities.

We have a diesel repair model. We include unavailability for testing and maintenance, independent failure probability. We treated this. You may remember on one of the earlier slides how we had generic designs and how we had a number of plants in each of the categories. We did an analysis, a generic analysis using average data, and we did it also on the plant-specific data for each appropriate plant.

(Slide.)

This is the distribution of the plants we studied, the reliability of the onsite AC power system.

It varies quite a bit. I'll go into the next few slides and show how a configuration and also some of the sensitivity factors apply.

Here the histogram shows average data that results for the configuration. Along the bottom I have configuration success logic versus unavailability. The bars show the specific plants, how their unavailabilities would fit under this curve. You can see that two out of three configurations lead to reliable configurations, but the worst one out of two would be worse than the best two out of three. So it's strictly not configuration you have to be concerned about. There are other plant-specific features that have to be considered.

MR. REITER: Chris Reiter.

The bars are averages?

MR. BATTLE: That's right. And then the -- the ranges of the specific plants we looked at.

MR. REITER: On the first one, wouldn't the average have to be somewhere in between the bars?

MR. BATTLE: This is not exactly an average. This is our generic model. In our generic model, we didn't give them any of the plant-specific common cause failure modes. They were just used -- we used the common cause failure probability that all plants are susceptible.

MR. EBERSOLE: Is that reliability in the context of starting and running?

MR. BATTLE: This is the initial unavailability, starting.

MR. EBERSOLE: What would it look like if it were running?

MR. BATTLE: It changes over time. I've got --

MR. EBERSOLE: Well, if it won't start it won't run.

MR. BATTLE: That's right. There is a contribution to the failure to run.

MR. EBERSOLE: So if I look at a 40-year plant life and look at the nominal regulatory requirement of two out of two, what does that tell me about the probability of a prolonged power failure per plant over its life? What are those numbers right quick? I can't fit them into my head.

That's 40-year life and you have an average offsite power failure of about once every five years?

MR. BATTLE: Right.

MR. EBERSOLE: How does this come out per exposure to a plant over its 40-year life?

MR. BATTLE: You're challenging it about eight times, I guess. So one of the worst plants up here would be 10^{-3} or more than that. It's -- if you look at the safety goal --

MR. EBERSOLE: That's no good.

MR. BATTLE: If you look at the safety goal of 10^{-4}, it does give you trouble.

MR. EBERSOLE: It doesn't meet it, doesn't come close to it.

MR. BARANOWSKY: Excuse me. The safety goal addresses core damage melt and risk to the public. This talks only about the frequency of being without AC power during the lifetime of the plant, emergency and normal AC power.

I might also point out that you might find that this plant or whatever that results in the fairly high unavailability of the AC power system could be coupled with rather reliable offsite power systems, so you don't want to make conclusions by putting averages in here.

MR. EBERSOLE: Right.

MR. BARANOWSKY: Let me add something else. The generic value is to essentially take the average reliability expectation for diesel generators and eliminate those common cause failure problems that were identified, at least limit them to some reasonable level that looks achievable based on plants that don't have experiences that indicate common cause failure problems. And one would then take those considerations and come up with this generic calculation of unavailability.

We might call that a reasonable expectation value on what one might get for unavailability for those given configurations. It is kind of funny that the plants with the least reliable configurations seems to have quite a few of the independent failures and common mode failure potentials, which is indicated by the fact that the bar with the spread on it falls above the generic value that we estimated, whereas those with the more reliable configurations seem to fall in the range of a generic estimate.

(Slide.)

MR. BATTLE: This slide shows something about repair and failure to run. I picked several plants. This is not generic data; these are specific plants. This shows how it changes. This is a log scale. You can see it does increase some more than others.

MR. BEARD: Is that spread at the top, is that the spread of the two out of three plants?

MR. BATTLE: This is a plant. We took plant-specific data for two out of three. These are two out of three plants.

MR. BEARD: So that one could be said the best two out of three plants or the worst two out of three plants; is that what you're trying to show?

MR. BATTLE: Well, no. I guess -- I think we only had two of these plants. These are the data we had for those two plants.

MR. BEARD: Let me ask a more fundamental question: What are you trying to say with the two curves marked two out of three?

MR. BATTLE: This is plant A and this is plant B (Indicating). It just shows the difference in how their reliability changes with time.

MR. BARANOWSKY: Let me answer that, too. Just because you have two or three diesels isn't necessarily an indication of how reliable your plant is. It turns out that you may have the exact configuration at your plant, but your operating history is such that your system reliability is much lower than what would normally be conceived for that configuration. I think that is an important point.

MR. DAVIS: Isn't one difference or couldn't one difference also be the LER reporting habits of the utility? I notice in your University of Dayton report they didn't have a very optimistic viewpoint on LER reporting requirements.

MR. BARANOWSKY: I think that would be true if you were looking at say total number of LER's. But when you are talking about what might be termed catastrophic failures of diesels that just plain simply don't work, I don't see how a utility could not report that without breaking some rule or regulation.

Moreover, remember that we sent a questionnaire out to every utility and asked them to take a look at various LER's we had to see if our interpretation of them as being failures or non-failures was correct, and for the most part they agreed, Ron, didn't they?

MR. BATTLE: That's right. There were a few changes. We added some and took some away because of the response, but it was nearly the same as what we got out of the LER's.

MR. BARANOWSKY: And that was a voluntary thing. I guess we sent the letter out to all and more than 50 percent responded, right?

MR. BATTLE: Right.

The next few slides are related to the sensitivity. It is very plant-specific, so rather than taking a number of plants and showing sensitivity data, we do have a little bit on some specific plants. Here I am trying to show what are important contributors to reliability and unreliability.

I took a number of cut sets in each category. Diesel undependability is the largest number of them, but it does not mean that it's always the most important. But it does appear to be. In a number of plants it is.

Human error is next; common cause failure, hardware common cause failure, and then service water common cause failure.

(Slide.)

MR. EBERSOLE: Would you go back to that curve of onsite system availability, that curve you showed? I'm trying to get a feel for why the two out of three systems appear to be intrinsically less desirable than the one out of two? That's contradictory to our current airplane logic, that doesn't let two-engine airplanes fly across the ocean.

Could you give me --

MR. BATTLE: Well, if you need two out of three diesels --

MR. EBERSOLE: Yeah, of course. It's a one out of three for the aircraft.

MR. BATTLE: If you just take it on that basis, it would be less reliable.

MR. EBERSOLE: So two out of three is intrinsically less desirable than one out of two. Well, sure, of course it would be. I had a mental block there for a moment. Thank you.

(Slide.)

MR. RAY: I'm having trouble reading your bar chart. I'm having trouble with the bar chart, understanding what it says.

MR. BATTLE: The one we just discussed?

MR. RAY: Yes. "Cut sets with importance greater than or equal to 0.2." What is 0.2, the unavailability?

MR. BATTLE: Importance is a measure of sensitivity, essentially. It's probably a little bit confusing to put the number in there, but I selected ones that -- I have the importance. It's a ratio taken of probabilities.

MR. RAY: So 0.2 is an unavailability?

MR. BATTLE: It's a ratio of probabilities, probability of a cut set over the probability of a top event. It tells you something about how sensitive the top event is to that cut set.

MR. CAMPBELL: I'm going to add a little bit to that. For example, on the human error common cause failure, what this says is that 7 of the 18 plants had greater than 20 percent contribution to the system failure probability due to just human error common cause failure. So if I take a look at one of those plants, then, you know, the human error common cause failure might be 50 percent of the total system failure probability.

The same thing holds for the other common cause failure events there. In the case of the diesel generator being undependable, of course there would have to be, you know, two or more diesels failing. That is the independent failures, combinations of those.

MR. DAVIS: Do the bar charts represent the number of plants out of the 18?

MR. BATTLE: No. There are some plants that have more than one cut set of 20 percent or more.

MR. EBERSOLE: Did you find a substantial number of plants had their own air-cooled radiator systems versus service water systems? What's the ratio there?

MR. BATTLE: I can't give you the ratio there. There are a few out there, four or five plants maybe.

MR. EBERSOLE: That use fan radiators?

MR. BATTLE: That's right.

MR. RAY: It's not the predominant design?

MR. BATTLE: Service water is, and they're getting more impractical all the time.

MR. PAULITZ: I have a question. Going back to that other curve you had of onsite system reliability versus time, aren't you really saying there, when you say two out of three, you are saying that is a two-unit station that may or may not have common offsite for both units, and most times it is, that if you lost it both units require at least one diesel? So it's really saying if they had a shared diesel that you need two out of three; is that what you're saying?

MR. BATTLE: That's right.

MR. PAULITZ: When you got down to one out of two, that could be a single plant sitting there with two diesels, needing one out of two. However, if it was a two-unit out of two diesels you're down to two out of four, aren't you? You drop the next curve down. You are mixing a little -- whether it's a single unit or a two unit, whether it's shared or not shared.

MR. BATTLE: The number of units really isn't that important. It'd make a difference in how many units you melt, but --

(Laughter.)

MR. PAULITZ: It's not a single unit requiring two out of three diesels. There may be some and there may not be; is that true?

MR. BATTLE: I don't know of any single units that are a two out of three configuration.

MR. BARANOWSKY: There are none.

MR. PAULITZ: I didn't say what they needed, but they do have two out of three. But this two out of three, does this represent a two-unit station, then?

MR. BATTLE: That's right. In typical configuration, these four diesels could be shared between the two units.

MR. PAULITZ: Could be shared or could be independent? If they were independent, it would be a one out of two configuration.

(Slide.)

MR. BATTLE: This slide shows a little bit more on the sensitivity on the configuration. One out of two plants, the diesel undependability and diesel common cause failure report, two out of three diesel undependability, diesel test and maintenance. It goes into the events that are important for these types of configurations.

The thing I guess I need to point out here, these are not always in this order. This is usually the order that it might meet this configuration. For other plants it has been switched around.

To show sensitivity, I would have to treat it on a plant by plant basis. I'm trying to summarize here what events are important in general. You take some plants, these will be switched around.

(Slide.)

This is another sensitivity curve for independent failure probability. It shows you how the unavailability increases for two different configurations. You can see for the two out of three, as the independent failure probability increases it goes up -- the unavailability increases much faster than for one out of two.

MR. KASTURI: I have a question. Earlier on when you said two out of three, you were primarily talking about a two-unit station. I'm not so sure there aren't units in here that are operating that don't have a three-bus configuration, that used to be somewhat in vogue in the early seventies, that doesn't have a two out of three for a single plant.

I was wondering, in those cases would your curves be kind of misleading?

MR. BATTLE: Well, if you find a plant with three diesels that we said was a one out of three plant and you decide really it's not, it's a two out of three, well, you can change. We have a methodology now.

When I started out, I tried to say that we are not analyzing a Hatch or we're not analyzing Farley or whatever. We are using them to use realistic data. But they may be different.

MR. KASTURI: I'm just sort of wondering, if one looks at this curve, that a single-unit plant with a two out of three unit configuration is inherently less reliable. I'm not sure that's not the impression you're leaving here. That may be just something you want to think about.

I feel if it's a single-unit plant and it's a two out of three configuration, the curve might look like something different.

MR. BARANOWSKY: No, it wouldn't.

MR. CAMPBELL: These numbers do not depend, really -- it's a mistake to be thinking about a number of units. This represents an AC power system and the success logic for that system. It's really independent of whether you're talking about one or two or three or any number of reactor units here in terms of the system reliability. We have defined the success logic for this system.

MR. KASTURI: There's an inherent fault in the logic of what you just said. The inherent fault is that in order for that plant with the two out of three diesel with the single unit to perform that safe shutdown it only requires two out of the three trains of the equipment operating, and there are plants that have the swing bus concept, that you inherently are -- do fall in the category one level above the one out of two system configuration. It's something you ought to think about.

MR. CAMPBELL: It would either be a one out of three or two out of three or one out of two. I don't know exactly what you're talking about. But in terms of doing a reliability analysis, you would have to specify a number of diesels that operate for successful system operation. That's all we're doing here.

MR. KASTURI: For a two-train safety injection system, if I can put -- for example, I know a plant which I was involved in, I put a B safety injection pump which can be started either on the A bus or on the AB bus, in which case its reliability is much higher than it would with the one out of two plants. At least intuitively, there is some fault -- I haven't done the detailed evaluation that you have done, but there is something that doesn't seem to add up in my mind.

MR. CAMPBELL: For a diesel like that, I guess what you're getting at is it would be more reliable in terms of its dependence on external systems, such as DC power service water, because possibly you could cool it with either the service water train or you could start with your DC power train.

In the cases -- well, like for the two out of three, even if that is a swing diesel that capability does exist. We did model that explicitly. The same thing with the two out of five. The odd swing diesel we always model as having the capability with either DC division or being cooled by the DC service water division.

MR. KASTURI: I think the clarification was offered that the two out of three was an inherent two-unit station. I don't believe that we should leave that impression here.

MR. CAMPBELL: I still do not believe that it makes any difference whether it's a one or a two-unit station, the way we've defined the problem here.

MR. BEARD: Ron, let me see if I can clarify something. I took the draft report and tried to study it. If I remember correctly, you look at the number of diesels at a given, I'll call it, station, just to clarify things. The station may have one or two or three units.

If for example they had five diesels and two plants, you made an assumption that, since you're not considering within the scope of this review the big break LOCA, that probably one diesel per reactor unit is sufficient to get the plant down. If I remember the report, that is the assumption.

MR. BATTLE: That's right.

MR. BEARD: Any time you see a failure or a configuration that has a number greater than one, by definition you must be talking about a more than one unit station, because you made the assumption.

MR. BATTLE: That's right.

MR. BEARD: Because you made the assumption you only needed one diesel to bring down the plant. Now, that assumption may or may not be good. But my assumption in the report is the two out of three is a two-unit station and the one out of two may be a two-unit station or it may be a one-unit station. It may be one of the plants at Millstone or it may be a single-unit plant, like Kawanni.

MR. BARANOWSKY: That's exactly right.

MR. CAMPBELL: That's right.

MR. RAY: I would like to make one observation. I'm convinced from this discussion and those that preceded it that you shouldn't play stud poker until you know how to read the cards.

(Laughter.)

(Slide.)

MR. BATTLE: This slide shows some of the similar sort of data that I've shown in previous slides, so I won't go into this slide much. It shows important contributors to reliability for different configurations, and then at the bottom of the table it shows actual studies showing different parameters. You see how the first two columns show how, say, the independent failure was changed and it shows the result of changing the onsite system unavailability.

Here there are no orders of magnitude changes. I have estimated some costs for some of the changes that would come out of the sensitivity study.

(Slide.)

On independent failure -- I'm giving some examples here. It doesn't apply to every plant. In some plants such changes would be useful. I'll show you some of the cost factors for these: to install air dryers and air start systems, it's about $100,000 a diesel.

Some of these recommendations came out of the Dayton report and we added some cost figures to it. E-9 Relay doors, $10,000 a diesel. A governor has a problem and a periodic overhaul might help that, and that's $6,000. Rewriting test procedures. If you have procedures that are going to cause common cause failure, rewriting them is about $5,000 a procedure.

Then we go into design feature. Common cause failure modifications are not terribly expensive. To add a diesel is like 20 to $30 million. So that's a big fix there. These numbers do not include reactor down time, which may override all of them, except possibly adding a diesel.

MR. EBERSOLE: Did you look by any chance at the unique problem of multi-unit plants as contrasted to single-unit plants in the context of whether you should design an integrated plant or simply two stalls with a unit in each stall as though they simply happen to be next to each other? Did you look at the merits of approaching the design from an integrated viewpoint?

MR. BATTLE: The only way I could look at that is we do have some two out of four reliability figures.

MR. EBERSOLE: No, I'm talking about beyond that scope. You see, in the one case you have an AB channel and system where the given channel has two diesels. In the other case you could actually have four channels, or you could have the two train systems having dual feeds, if you want to look at it that way, where you treat the central station of four units as a central feeder to the two-unit configuration of each unit.

There's a distinct difference depending on how you look at the station.

I am convinced personally that the unitized design is not as good as the integrated design.

MR. PAULITZ: If you have an integrated design, you are going to have exposure of both beyond a given unit.

MR. EBERSOLE: True.

MR. PAULITZ: You may have more problem than benefits. In looking at the reliability, you could say, yes, this configuration numerically is going to be better. In the real world it may or may not be. Those are some of the problems.

Now, in the case of that air dryer, the real problem was moisture. It could have been taken care of at zero dollars if people would have drained the tanks properly and periodically. Obviously, they haven't done it. Some of the reasons they don't drain the tanks has never been looked into. Why do some utilities have the problem and others don't, with or without air dryers?

Some compressors run more often because you have air leaks, and you're going to find more water or moisture in the receiving tank. That's some of the problems. Others is the common -- at the bottom of each tank you'll find a plug valve. Some of them are not interconnected. They are right next to the floor. You put a wrench on them, you turn it, the water hits the floor, comes right up and gets you in the face, 200 pounds. Well, you're not going to go back for seconds.

So a lot of it has to do with design, training, and procedures. Electrical substations inherently have compressors. Almost every substation is full of them. And the older ones, they are all air compressors. Every breaker had its own air compressor. Yet they went out there every day and they blew the water out of them. They blew it to the point where they didn't see any more coming out.

They also knew when they saw a lot of water coming out that this thing's got a lot of leaks and they go fix it. So yes, you can fix a problem many ways, $100,000. You can fix it other ways a lot cheaper, too.

MR. BATTLE: We looked into ways of removing moisture and we had particularly --Hanover's Dayton report sent out the questionnaire. They responded to how they removed moisture from their compressed air, and almost all of them at the time used blowdown. I don't know if they actually did it, but they said, this is what we do. So the problem still exists, in spite of the fact that almost every one of them said that they did that.

MR. BEARD: This afternoon when we give some of the staff's experience with operating reactors, I am going to specifically address unitized design or station design. So I don't know whether what we have to say will address your concerns.

MR. EBERSOLE: I'd just like to see a comparative analysis of what you do on a three-unit plant. Should one view it as a three-unit plant or simply three stalls?

MR. BEARD: We have some comments for this afternoon.

MR. CAMPBELL: Also along those lines, the way we analyzed Farley was, for all practical purposes, as a unitized plant. Because what we said is, they need any two out of five diesel generators.

MR. EBERSOLE: When you say unitized, that could be two things: unit by unit or integral.

MR. CAMPBELL: Integral. We said they need any two out of five diesel generators. They have four separate trains of service water. We said, okay, any two of those, and we can align the proper train with the proper diesel. The only thing we didn't do as an integral plant there was, you know, four divisions of DC power, and it turned out in most cases that DC power was not a major contributor.

So like I say, for all practical purposes that was analyzed as an integral plant.

MR. EBERSOLE: Well, the NRC now has almost an edict against integral designs. It's almost a requirement.

MR. CAMPBELL: In doing that with Farley, we did give them a lot of credit for supplying the right loads with the right diesel and connecting it. They had two diesels normally aligned to Unit 1 and they said, well, we'll make this cross-connection and align the second one to Unit 2. So it's really not designed that way, but we did analyze it that way.

MR. EBERSOLE: Thank you.

(Slide.)

MR. BATTLE: I will conclude. One point I guess I would like to start out with that's really important in the results we found is that reliability is plant-specific. There is no fix that you can do with the industry.

Some of the fixes that do exist at some of these plants that we have looked at -- I want to look at some of the cheaper ones -- were improving test and maintenance procedures, improving maintenance procedures primarily. This is cheap. You get some improvement in reliability. It's not a big improvement in most cases, but you do get some.

Where common cause design features do exist, they can be eliminated, most of them, fairly cheaply. Some plants have high independent failure probability. If they do, and particularly on some of the less reliable configurations, they can fix their independent failure probability and improve their own site system reliability quite a bit.

We have identified some of the failure modes that can be repaired and worked on. Dependence on other plant systems, service water and DC, are important in some cases since the diesel is dependent on both of these. If their unreliability is high, it's going to make the diesel unreliable.

Some plants perform excessive schedule maintenance. The average was quite low, but there are some that are way up there, and if they can reschedule that without reducing the diesel reliability itself, which some seem to do, they can improve their reliability by doing that.

That concludes it.

MR. RAY: Are there any questions for Mr. Battle from the panel, from the audience?

MR. BARANOWSKY: Could I add one thing about the improvements? Even though Ron identified the cost of some improvements, I think the gentleman from Stone & Webster had a good point about any individual plant might be able to fix a plant in a different manner at say much less cost to that utility. Therefore, all we really want to do is identify the problem area. And when people identify their systems as operating unreliably, we would suggest that the licensee propose the design, not the people sitting back in Washington, D.C.

It is our job to review the kind of things they do against appropriate criteria, but the nature of the fix is really something that's dependent on the nature of the plant's design.

MR. RAY: You're going to diagnose the problem, but you're not going to prescribe the treatment.

MR. BARANOWSKY: We're going to identify the problem areas.

MR. RAY: That's what diagnosis is.

MR. BARANOWSKY: And we're going to suggest that requirements be developed, that one will be able to determine through appropriate monitoring that they have in fact achieved an adequate level of reliability. In other words, their failures and so forth.

MR. RAY: Well, at this point in the program we were scheduled tentatively to have a general discussion, but in view of the fact that we have been rather exhaustive in our questioning of you I think I would rather declare a one-hour lunch break and start the noon session with with the discussion on this morning's presentations.

I assume that everyone on my right will be here for the afternoon's session and I know the panel will, and I would invite those of you in the audience who would like to participate in the general discussion of what transpired this morning to come back. You will have your opportunity.

So we will come back from lunch at 2:00 o'clock.

(Whereupon, at 1:00 p.m., the meeting was recessed, to reconvene at 2:00 p.m. the same day.)

AFTERNOON SESSION

(2:00 p.m.)

MR. RAY: We will resume the meeting, please.

I would like to advise anyone in the audience who didn't have an opportunity to get the handouts this morning, we have some extra copies which we now have, and you are free to take one.

I would like to open the floor for general discussion on the part of the panel, the NRC representatives, the Sandia or Oak Ridge or members of the audience who have an interest in what transpired this morning and feel that they are in a position to make some constructive comments, to invite them to do so. Is there anyone who wishes to volunteer as the lead man?

(No response.)

MR. RAY: Walt, or Ep, or Pete?

MR. EPLER: Well, I observed that we have some problems that are hard to fix. Diesels are almost as good as they are going to be. I gather that in fact a factor of two might be anticipated, but if you have to make 100 starts to prove you have a factor of two, you already diesel out, so I am not sure we are going to get much proof. So, I think maybe it is time for us to ask, what is the appropriate distribution of effort between events that happen frequently and events that happen infrequently, and this relates to testing diesels with a fast starter.

It is a highly improbable need, but it is impacting our frequency need. You could say the same thing with respect to AC and DC. Why do we have to have reliability in a system in which it is so hard to get reliability? Well, it is probably partly for improbable events and partly for frequent events. Well, we can fix the frequent events. Technically, there are ways. And the frequent event is being forced into shutdown heat removal, and when you are forced into that mode of operation, we should have a mode of operation which we do not have, and that would take care of many of our problems.

So, what I am saying is that I learned this morning that we are now facing problems where we can make no further substantial progress. We have over 30 years of experience with these systems, and I think we have learned something, that we failed to put in a system optimized for removing a small fraction of residual heat, and it would be a lot more cost effective to fix that than to try to fix everything else in the plant which cannot be fixed.

Do I get an argument?

MR. RAY: So if I could put this into my interpretation of your comment, we should not worry about trying to make the diesels more reliable. We should go all out for a dedicated residual heat removal system.

MR. EPLER: I don't like to be quoted as saying we shouldn't worry about it. I would rather say that it would be more cost effective to take the other course and put in an independent protective system where you could walk away from the plant and expect the heat to be taken out, and take care of big fires, many acts of sabotage, and other things that we cannot do much about, and it would not exacerbate the public's perception of risk, as is now being exacerbated.

MR. RAY: Well, perhaps the unresolved safety issue, A45, will prove in a dedicated heat removal system.

MR. EPLER: We have a report from Sandia which leads me to a different conclusion, that it is not cost effective to make improvements specifically to aux feedwater, that the improvements would be fractional, like 50 percent, not even a factor of two, except in one case. I recall you could get a factor of eight by alerting the operators to certain events and training him to respond correctly. Now, if you had a system that could be improved that much by a low grade operator, it must be a poor system.

MR. RAY: Does anyone have any contributory remarks supplementary to Mr. Epler's comments, Epler contrary?

MR. BEARD: This ought to pre-empt what I was hoping to say in a few minutes, but I think in general I agree with the comment for the most part. On the average, the plants look pretty good insofar as diesel reliability goes, but there very well may be some outliers where significant improvements could or should be made. I think my personal opinion is that that is where we should focus our attention, in the outliers.

MR. BARANOWSKY: I might second that on the whole issue of station blackout. I was trying to say that a little bit this morning. That is to say, there are probably some outlier problems that one needs to address in a reasonably expeditious manner, but when you talk about making overall industry improvements in reliability or improving core damage frequency reliability, you are talking about systems and concerns, and an integrated approach is the way to go on that.

Therefore, I would not propose a station blackout fix on the average for the industry. That would be better addressed in another form which looks at all the problems together and determines an optimum way to address what kind of systems or modifications would be required. I don't want to say that we are going to let the high risk outlier type of problems slide in the interim either.

MR. EPLER: I would like to observe that we have three problems, three problem areas. We have between one and $200 billion worth of plant out there, and we do not have options for what to do about them. We can patch them, maybe not in optimum fashion, but we could change them at some great cost. Those in the pipeline we have a great deal of uncertainty about what we can do, not about future plants. Are we going to build future plants like we have now, or are we going to do it better? We should be talking about future plants, because some day we may get one, and surely we have learned something in 30 years. Why don't I hear more about that?

MR. LIPINSKI: In terms of what we have learned in 30 years, the BWR boiling water reactor that included high pressure boric acid injection in the event the control rods did not scram has a diverse method to shut down. Given that you shut down and you lost all AC power, there was a dedicated residual heat removal system that took care of that plant.

MR. EPLER: So what did we learn?

MR. LIPINSKI: I am just telling you what we have learned, not to include those basic features. They are not here today.

MR. EBERSOLE: Mr. Chairman, may I make a comment?

MR. RAY: Certainly.

MR. EBERSOLE: I tend to react to the loss of all AC power as maybe being somewhat as serious as it is. The implication here in some of our discussions was that so if that occurs, all is not lost. We have aux feedwater and a bit of DC to run it for one or two hours, and somewhere beyond that there is a capability, but I guess a lot of that went by me, because I haven't yet seen a design, although I don't know why I shouldn't see one, which has got a simple reliable steam driven turbine feedwater pump and associated mechanical pneumatic, hydraulic, or you name it, as long as it isn't electric facilities with which to monitor my course of action and see if I am maintaining myself in a safe state.

I know of no such designs as that, yet it was implied here that I can in fact go beyond the battery kill level and somehow keep going. I wonder where that information has been found.

MR. PAYNE: Arthur Payne, Sandia Labs. In talking with people at Terry Turbine and GE about their pumps, when we say that operator probability of bypassing DC is up .5 . There is a place like Calvert Cliffs where the aux feedwater will continue to run without any operator action whatsoever, just continue to run as it was when they lose DC power. It is a mechanical governor on that.

MR. EBERSOLE: How did they go not overfilling the boiler and checking themselves out of existence?

MR. PAYNE: We are talking about four hours into the accident. Decay heat has dropped off. It is kind of leveling off now. And the turbine is throttled down. So when we finally lose level indication, it will take several more hours for that to fill up the steam generators and to cause the steam turbine to fail.

MR. EBERSOLE: Is this to say that there are plants that in fact can operate beyond the DC power failure point, and we have some demonstrable literature that I can read that tells what people do under these circumstances?

MR. PAYNE: I think the idea is that at Calvert Cliffs they don't have to do anything, that the machine will continue to run. Now, if they wanted to keep it running for innumerable hours, they will have to have some method of deciding what the steam generator level is and whether they should throttle it down. Now, if you wanted to, you could have a procedure to throttle it down so much every hour depending on the decay heat curve.

MR. EBERSOLE: In the meantime, I don't know what the decay heat levels are.

MR. PAYNE: No.

MR. EBERSOLE: I don't know what the primary loop condition is. I don't know whether to call for evacuation of the community or not and kill a lot of people.

MR. PAYNE: Well, I think you would know that if things got to that point already.

MR. EBERSOLE: In short, I have got nothing in my context of need. This is illusionary, and it is all claim.

MR. PAYNE: Well, I think there is some probability that these things will continue to run.

MR. EBERSOLE: Yes, and it is low enough not to warrant any significance at all, because I don't see any evidence.

MR. PAYNE: If you look at the sensitivities we did, you will see that this is not a particularly significant part of the problem.

MR. EBERSOLE: Going to the battery degradation point, I think we have to do something different. I don't know what it is, but it is not claimed continuity of action after that.

MR. BARANOWSKY: I think if the accident risks and likelihood associated with sequences that involve batteries going beyond their capacity, if those things are high enough, then one has to take a closer look at that assumption. In fact, probably what has to be done is either battery capacity has to be increased, or some of these fixes which involve having some independent capability of providing charging power for instance to a battery has to be added.

I don't think the NRC would go along with assuming that that accident sequence is unrisky just because the turbine will keep on running. It happens to be a little bit extra that we look at so that we can give as realistic a perspective as possible, but not something we want to hang our hat on.

MR. EBERSOLE: Okay.

MR. RAY: My wife tells me repeatedly that I am a natural born optimist. I think we have an asset here that we are not giving due credit to. I don't know how the Commission could do it, but that is the operator and the operation management. When you are reaching the point, I still maintain, when you are reaching the point where battery life is in the balance, I cannot believe that the management of that plant is not going to get some sort of DC generation into the plant or AC supply to the charger into the plant to restore the capacity of the battery, and if that is the life preserver we need, I think forms wherein the operating people participate and representatives of utilities should certainly emphasize that point, if people who are running the plant in spite of the mistakes that were made at TMI and elsewhere still are an asset and are thinking about the problem, and they are going to resort to expedients that aren't in the plant to help them bail out of their problem.

I know you cannot prescribe that in any regulatory sense, but it is there. So, I am inclined not to take as dubious a viewpoint as I have heard from several people here this morning.

Let's get back to the presentations this morning. It is true that maybe a dedicated heat removal system is a better solution to the blackout problem, but the consensus of evolution in the NRC realm and the ACRS deliberations hasn't reached this point. The fact is, we still live with the diesel generators as they resort at loss of power, and we have an analysis presented this morning on blackout, and I think those are the things I would like to address with commentaries in the next few minutes. One, Pat Baranowsky outlined for us again on an updated basis the mode of approach or strategy, if you will, of addressing the unresolved safety issue A44, station blackout. Do we have any comments we would like to offer on that strategy?

MR. DAVIS: Jerry, could I make a couple of remarks on that?

MR. RAY: You bet.

MR. DAVIS: I was also going to express my concern about the fact that there might be some outliers out there, and I was happy to hear they are going to be looking for them. There are enough variabilities in how one procures and designs diesels that if you stack everything in the wrong way, you would have a lemon out there that was waiting to have a problem.

I would also like to encourage the plant visit. There is just no substitute for walking the lines in the plant. In fact, my experience has been that you cannot find dependent type failures by looking at PNID's. You have to go to the plant. I think that is one thing that is essential in a study like this.

My last point, it seems to me like there is not enough involvement between the utility and the diesel manufacturer. This seems to come out in the University of Dayton report, and I found it to be the case in some experiences I have had. Let me tell you about one case. I know of a plant that was having trouble with overspeed trips on their diesel. This wasn't a diesel generator. It was an aux feed diesel driven pump. So they merely set the overspeed trip from 1,100 rpm to 1,300 rpm. The problem went away. Reliability became very good. But I happened to be talking to the diesel manufacturer some time later, and he said they never should have done that. The unit was not designed for operation at that speed, and that sustained operation at that speed would destroy the unit.

So, this, I think, illustrates my point that the manufacturer should get cycled into some of these things, or we are going to have a problem. No one should know more about the diesels than the manufacturer. And I do not think we are relying on this experience enough.

That is all I have.

MR. BARANOWSKY: I think for troubleshooting diesel generator problems again I would like to emphasize that we are not claiming that the NRC should propose fixes. If there is a problem, that needs to be worked out by the people who know their machines best, the utilities and their manufacturing representatives. So I agree with you completely. There are other cases in addition to the one you pointed out wherein I know some so-called fix was made that ended up damaging the machine.

MR. EBERSOLE: I would like to make an observation about Jerry's happy view on the DC system here. If I take a case of the minimum configuration -- which is two rectifiers, I believe, and two batteries -- I face inevitably the day when one rectifier will fail over a forty-year course. Then I am left on one. I am left on the reliability of that rectifier to stand in there, and since it does not experience a surge or anything else, its steady state is an influence, then it should be pretty good.

It is only now the intrusion of a random event in the interval where I repair or get a new one. People will be super nervous, or at least they should be under the circumstances where they are held up by one link in the chain for an indefinite period.

I would like to have, Pat, you investigate how fast people would have another rectifier into service and what is the period of exposure on one train. Remember, it does no good to shut down. In fact, it may compound the problem.

MR. BARANOWSKI: Right.

MR. EBERSOLE: And I do not think even some prudent utilities might have a half a dozen in a warehouse somewhere, but I am not sure that is true. My experience has not been you can get things done all that fast, even with helicopters.

MR. BARANOWSKI: I think usually there is a spare.

MR. EBERSOLE: Is there a requirement?

MR. BARANOWSKI: I would rather have someone from NRR address what the requirements are on that, if there is such a requirement.

MR. RAY: Is there anyone from industry here who would like to respond to this point?

MR. MAC AVOY: Some plants have an installed spare that can be put on either buss, but that is not common. Usually the plant just has one rectifier and one charger per buss. If they have a spare in the warehouse, that is their business.

MR. EBERSOLE: Like in two systems you are hanging on two trains. They are both running. You have got to have one. Inevitably you are going to have just one and then that is where the interesting point comes. How long will you be on one and what become the pressures while you are on just one.

If there is any incremental loads, that is a factor that degrades the single system that remains, but I do not think that is true in that case.

MR. MAC AVOY: I think you are into a tech spec area once that happens. The utility, if they are smart, whenever they have a tech spec-related device, they will have a spare one that they can install immediately.

MR. EBERSOLE: The same goes for the inverters, except they usually have accrued AC power source available after breaking the continuity of the AC service. But they usually have an extra over and above the inverters.

MR. BEARD: Could I provide some more information on that? It has been my experience that we in the NRC especially tend to focus our attention on the equipment that is in the plant that is so-called safety-related for obvious reasons. But sometimes I think we get carried a little overboard and we tend to forget the equipment that is in the plant that is not safety-related.

I believe some of the plants out there have other DC systems for other purposes that are not safety-related and if a battery goes down south, they are going to go over and pull it off and get a charger and get it on there. Now it may not be seismically-qualified and it may not have a flood of paperwork to show it is pedigree, but it probably will work.

MR. EBERSOLE: You might get one out of the turbine hall.

MR. BEARD: That is a pretty good shot.

Let me carry the same point one step further or into a little bit different realm with regard to the inverters that you brought up.

Someone mentioned, I believe, this morning that the worst case was like two inverters and two, I will call them, raw AC. They are not really raw, but they go away when the power goes away. The probability that you will lose the regulated AC and hence lose some instruments and so forth and so on, I think, was presented.

It has been my experience in dealing with operating events, the real things that happen, that that is not the one that you have to worry about. The one that is a more frequent occurrence, which I am sure you are familiar with, have been the situations where you lose part of the instruments, part of the power, and maybe some of the instruments even fail to mid-scale readings, and what you end up with is a situation where the operator has, say, three or four channels and they all read different, and he says my goodness.

So it has been my personal belief that you do not have to lose all the instruments and go blind before you have a problem.

MR. EBERSOLE: You get contradictions right away.

MR. BEARD: After all, he is only a human being.

MR. EBERSOLE: The other thing, when we ran these probabilities out to 10^{-4}, I recall some recent meetings and discussions we have had which seem to indicate that if you get out that far, I mentioned the common mode influences, you are in the regime now, I think, where the exceedance -- not the occurrence of just a low level earthquake but the exceedance of the design basis earthquake -- is in the same realm of possibility, which acts as a cutoff to your numbers beyond 10^{-4} or thereabouts.

Beyond that point, it is dark because what you claim is 10^{-5}, 10^{-6}, 10^{-7} is automatically cut off by exceedance levels of earthquakes. So the cloud comes down on you and those numbers are not very meaningful.

MR. BARANOWSKI: I think the capability of a plant to handle a design basis or greater earthquake is something that is now being looked at at least from a research point of view at the NRC. There is a program -- I think it is called the Seismic Safety Margins Research Program -- which would address that kind of thing.

I think we are now going to just start factoring that kind of thing into our probabilistic and risk analyses, whereas over the last few years when you look at the IREP studies in particular, that was left out. We did not think we had the technology available at that time. We were talking about in the Office of Research developing what we think might be a somewhat standardized method to better analyze those problems, especially in light of the results that came out of the Indian Point risk studies.

So there is some agreement there.

MR. RAY: I would like to get back to the question of what we think of the strategy and methodology that was elucidated on A-44 manipulation. What do you think about that study? If no one is going to stick out their neck and lead, I personally think that the outline that Pat gave us this morning indicates a very comprehensive study and a workmanlike approach to the problem, and I am very much encouraged by the indication that the philosophy that will orient the message to the licensees is going to leave the door open to them to engineer the solution, subject to the approval of the NRC Staff.

I think that is the intelligent way to go. I commend you, Pat, and those of your organization, for endorsing this. I think it is a trailblazing approach that would very well be implemented in many other of the NRC areas of concern.

I do not know whether the rest of the Committee will endorse this thought, but I, for one, feel that we should encourage or commend the effort as to quality and methodology and wish you well with it. If there is anyone on the Subcommittee who wishes to offer a demurral, the door is open for you.

MR. EBERSOLE: I concur with you.

MR. EPLER: Right.

MR. RAY: Now how about the outline that Sandia gave us on their analysis this morning? Are there any comments that anyone on the panel would like to offer on this?

(No response.)

MR. RAY: Well, here again I think that if one considers what could be done in this area that it is a workmanlike approach and it looks like you anticipated most of the areas of concern and it seems to me that you have tapped the experience available in the industry to useful purposes.

I think the laboratory that the operating plants represent is certainly an invaluable source of guidance and we should take that experience and convert it into terms that are interpretable and useful from analytical viewpoint to determine where are and where we might go. I personally can offer you no comments to change your approach or amplify it in any way.

Is there any other comment that anyone would wish to offer on this analysis?

MR. EBERSOLE: Jerry, the only comment I had I think I already made, that the curtain does come down before you get 10^{-5} or 6, and that 7 and 8 and all these other numbers just put a bankrush over that.

MR. RAY: What you are saying is that these numbers are not holy.

MR. EBERSOLE: They do not consider the real world.

MR. RAY: Do you have any suggestions that you might make?

MR. EBERSOLE: Just to make some observations that at this point the influence of common mode effects such as earthquake, if you wish, begin to override and, therefore, these numbers are academic beyond this point. Give it some realism or some such thing as that.

I mean, you know, qualify the meaning of these. I have seen GE and others come out to 10^{-14} and these numbers that you cringe in your seat.

MR. BARANOWSKI: I think you will see no 10 in any study that I have anything to do with. I would also like to have you note that the Sandia people did indicate that earthquake common mode failures can occur at frequencies like 10^{-4}.

Maybe we need to bring that out a little bit better in our report, to qualify the results to say you can bring all the other things down to 10^{-6}, if you believe you have them all identified, but there is still that other item which I do not know if we are ever going to be able to have confidence in frequency estimates of less than 10^{-4} or 5.

I would have to ask the seismologists that one.

MR. EBERSOLE: Your pitch, Pat, was to consider the integral problem and when you do that, that frequently disables the singular numbers on particular topics.

MR. BARANOWSKI: But I think we can do things like having a regulatory requirement that addresses the non-seismically-qualified equipment failure interaction with the systems that are required to mitigate that kind of an accident I think for the most part on the new plants that is pretty well handled.

But this program is designed to take a look at the plants that are operating and then I think you will find a spectrum of considerations there, not to mention the fact that people do not necessarily know the weak link in their plant when it comes to a seismic event.

I think at Indian Point when they found out that the ceiling in the control room might come down on the operators, they were not so much worried about tanks and other things collapsing.

MR. EBERSOLE: Well, one of the more recent things I noticed that bothered me, it has been found that the 250-volt DC casings are cracking as they sit there. They have tried to track this down in the one instance I have heard of -- and there must be more than this -- and they have concluded that what is happening is a subtle thing, where on a cell-by-cell basis the design of the battery looks perfectly competent seismic-wise and so forth.

When one bolts it together with rigid bus bars, it becomes a new structure capable of imparting new loads not heretofore identified on the cells and the casing and perhaps even the slightest shake will crack the cases and drain the electrolyte out cell-by-cell, and you do not have a DTC when you need it -- the worst.

So the subtle weaknesses have yet to be

dredged out.

MR. BARANOWSKI: And that is one good reason for making sure that the NRC programs take into account what we have learned and observed in some proper fashion, and we have an office in the NRC which is supposed to perform that function. It is a very important function.

MR. RAY: I would like to go back to Jesse's point on the fact that the probability of earthquake incidents and the results are of concern for station blackout perhaps. Maybe so, but the fact that you have analyzed the station blackout and the dependency or undependability of diesel generators to at least eliminate these as the controlling criterion of events is a point of progress. So now we can concentrate all our talents in deciding what to do about seismic concerns.

I would like to open the door to comments anyone would like to make about the Oak Ridge presentation. I would myself venture the thought similar to my comments on the Sandia work that this is a contribution to progress from the viewpoint of knowing what experience indicates.

Would anyone in the audience like to make any comments at this point?

(No response.)

MR. RAY: Okay, we will get back on the program. I would like those of the principals who are participating in the presentations for the rest of today to resort to any brevity of presentation that might save us a few minutes because we are roughly 40 minutes behind schedule and I would like not to go to 6:40 tonight. The schedule says 6:00.

But, on the other hand, if there are any earthshattering revelations that any commentaries will bring out, we will not overlook the opportunities. So do not feel so inhibited.

Okay, Mr. Beard, I think you are the first man on the program.

MR. BEARD: My name is J. T. Beard and I am in a branch of NRR that is called Operating Reactor Assessment Branch.

(Slide.)

We have a slide up there that sort of gives the title recent experience with diesel generators. I would like to say just as a way of introduction that the comments that I am going to present here today are those of our branch. They are not necessarily in total agreement with everybody in the NRC.

Let me go on to the agenda here.

In the agenda, I would like to say we are going to talk a little bit about where we are coming from, what our sources of information are, and leading up to the last item, comments. We will talk a little bit about some of the significant event that have actually occurred in operating reactors, and we are going to talk about some of these emergency tech spec changes we have been involved with that were mentioned briefly, a little bit about what types of failures, what pieces of equipment, etc., and comments, and I have tried to divide these comments up into four areas, just to give you some categorization.

I would like to say for the sake of brevity and in order to accomplish the major objective that I've tried to shoot for today, everything up to the last two categories is background. Now, we will be covering some events, and I know we will all be tempted to want to get into the details of what happened when all the diesels went dead, etc., etc., but that is not the primary objective today. That is just to let you know what has been happening recently, and set up the stage for the basis for the comments that are at the end.

(Slide.)

MR. BEARD: Okay. Under sources of information, where we are coming from, the talks that you have heard this morning have been prepared to provide the results from analytical studies, statistical studies, etc., things like LERs, License Event Reports. What I am talking about this afternoon has nothing to do with LERs. It has to do with day by day operating occurrences that are more or less in a real time sense. We have a phone call every morning with I&E. We get a daily update on what happened overnight, and this amounted to, I guess I have indicated here, over a period that is indicated there, about 2000 occurrences that have been discussed or reviewed over the telephone. Of those 2000, our judgements have indicated that something like 200 were of some significance in the sense that those were brought up to the NRR operating events briefings which are provided weekly to Mr. DSenton and to all the directors of all of the divisions within NRR.

I woud point out at this time that that includes the Division of Safety Technology who are in the business of developing and grouping new requirements. So there is an inherent feedback process in there of operating experience on the new requirements.

The point here is that some number, between seven and nine of these 200 events that were judged to be significant, involved diesel problems. That is a number like 3 or 4 percent of the significant events. There are a lot of them.

The second area we have experience in is on these emergency tech specs. I have just listed a few of them down there. There were three in Farley in '81, Peach Bottom, Hatch, Brunswick, Palisades. The Palisades item is on the wrong page. We will come back to that in a minute. But we are coming from a real operating experience, not a review of somebody's computer input report to that.

(Slide.)

MR. BEARD: Okay. This, we are going to go down through about seven or eight of these events real quickly. The Millstone event in January of '81 which caught a lot of attention, there was a human error which caused loss of DC. The reason we bring it up here is because it had an impact on offsite power, ordered start of the diesels, and what's more important, after the diesels were manually cracnked up, one dies from mechanical failure. The other one died as soon as they turned the DC back on.

While we are here, could we flip back and get that last one? This is probably as good a point to get it as any.

Palisades was a similar thing. Both DC systems were disabled for one hour, not DC systems, excuse me, both batteries were disabled for one hour due to a common cause event, and basically the plant was running on the chargers. The significance of this one at Palisades was had there been an accident, the automatic starting and loading of the diesels probably would have been jeopardized.

(Slide.)

MR. BEARD: You will have to forgive us for this out of sequence thing here. Again, another event at Millstone, it was discovered in the process of reviewing some information, not a real event, but it was discovered that there was a single failure potential of a breaker position relay that could have prevented the two diesels in Millstone from tying into the four KV buses. They would have come up, but they would have closed the buses due to a single event.

At Hatch during a test, two undervolt relays failed, and because they failed, the buses thought they had voltage on them. The diesels thought the buses had voltage on them so they wouldn't tie in.

At Dresden, Dresden is the two out of three situation we talked about this morning. There are two units, two reactor units, that is. There are three diesels. One of the diesels dedicated to each of the reactor units, and one is shared. What happened was for Unit 3, the dedicated diesel and the shared diesel between the units tripped during the test. It turns out they overheated. They thought it was air binding. They went through and did some studies and put it back on. The same event occurred the next month, October '81, on the No. 3 diesel. It turns out that when the unit tripped, they looked into it a little more deeply because it was a repeat occurrence. The problem they found was loss of cooling water, but it was due to loss -- defective check valves. They went back and looked at all the other diesels, and sure enough, they all had the same disease.

(Slide.)

MR. EBERSOLE: May I ask a question?

Do the diesels normally use an interposed cooling loop of cooling water, or do any of them use a jacketed water, or do you have a mix of these?

Do you follow me?

MR. BEARD: I follow you, sir. I just don't know the answer.

MR. EBERSOLE: Does anybody know? Do they commonly use an interposed cooling loop of cooling water through the jackets?

MR. KASTURI: Not always.

MR. EBERSOLE: Some use water through the jackets?

MR. KASTURI: Normally it is a closed water cooling loop.

MR. EBERSOLE: Right.

Do the ones that use raw water have problems with Asiatic clams and all that stuff, algae?

MR. KASTURI: I can't answer that.

MR. BARANOWSKY: Some do.

MR. EBERSOLE: Do they shoot them with chlorine?

MR. BARANOWSKY: They are looking at a couple of different things.

MR. CAMPBELL: Yes.

Well, in fact, we found one event I believe it was at Millstone where the act of shooting them with chlorine actually caused a failure of the diesels because all of the clams came loose and blocked up in the heat exchangers. But I am not sure I understood the answer to the first question. We are not aware of any diesels that use raw water like service water into the jacket of the diesel. There is always a heat exchanger and the cooling loop is separate.

MR. EBERSOLE: I understand there are some that way.

MR. KASTURI: It is one thing to say raw water and it is another to say raw sea water which I didn't mean.

MR. EBERSOLE: River water?

MR. KASTURI: Your question was were you always using treated water, and that is not always the case. It is not always treated water.

MR. EBERSOLE: It may be water out of the river?

MR. KASTURI: It may be raw water as it is called.

MR. EBERSOLE: Okay, thank you.

MR. BEARD: Moving on now to the next page, we have two of the more interesting events.

Calvert Cliffs, in June -- Calvert Cliffs again is one of these 2 out of 3 setups, two diesels and two reactor units. They ended up with temporarily loss of all diesels at the station, partial loss of offsite power. There was one line remaining.

The thing I would point out here is the reason the utility got into the setup was that while Unit 1 was down they took the diesel out of service for routine maintenance, and as someone said this morning, it was spread out all over the floor. It was not in a recoverable situation quickly. Then, while one of the diesels was down, they decided to take the offsite startup transformer, if you will, for Unit 2 out of service because it was due for its annual painting. The reactor tripped, the aux transformer was of course not available. They went to offsite. It wasn't available. Two diesels started up. What happened was the sharedi diesel tripped because they have had a chronic problem at that station with that diesel on regulators, and the second one tripped because the load dispatcher for the system called up and asked them to raise the output voltage for the main generator. They did. The reactor load coming back into the diesel tripped the diesel.

This, by the way, just a side matter of information, I understand it is being proposed as a potential abnormal occurrence for the Commissioners' consideration.

MR. BATTLE: Why were they paralleling the diesel to the offsite power system?

MR. BEARD: The unit was still up and they had, let's see, what was it? Is there someone back there who maybe has the answer more completely than I do?

MR. BRINK: Philip Brink with PG&E.

Once we took our transmission line out of service, by tech spec we had to exercise our diesel, and when we exercise our diesel, we have to load it, which means paralleling it, okay? That's why it was parallel to the system.

MR. BARANOWSKY: What would have happened if there was a loss of offsite power? Would that diesel have been able to start up and load emergency loads?

MR. BRINK: As it turns out, it could have been started back up. What operated was the loss of relay, and it actually just tripped the diesel. That relay is only operable when the diesel is parallel.

Yes, if we would have lost offsite power, we could have started the diesel back up and it would have sequenced the loads back on.

MR. BEARD: In fact, that's what you did. As I remember, in being involved with the event, as I remember, the diesels obviously didn't stay in a tripped state for very long. One of them was returned to service, reset and restarted in something like 15 minutes, but before you could legally declare it to be operable, you had to run it like for 15 minutes. So in the tech spec it was out of service for something like a half hour.

MR. BRINK: Yes.

MR. BEARD: But it was started by manual means in a reasonable period of time, something like 15 minutes.

MR. BRINK: Yes, I believe that is correct.

MR. BEARD: I am not trying to mislead you when I give you these descriptions of the event because I am trying to highlight what happened to the diesel. I am not trying to give you all the systems aspects of it, the fact that it was recovered, etc., etc.

MR. RAY: That's understood.

MR. BEARD: And I don't mean to slight any of the utilities.

MR. BARANOWSKY: Has there been any mechanism identified in this event in which this type of operation could have caused a loss of the remaining offsite power circuit through some interaction?

MR. BEARD: Not that I'm aware of.

MR. BARANOWSKY: And if that is the case, I guess I kind of wonder why that is an abnormal occurrence. I can understand the Dresden failure as being an abnormal occurrence, and maybe even the next one, but this one here sounds like it is just a not well thought out requirement for demonstrating diesel operability, and it doesn't seem that this failure of two or three diesels would occur under accident situations.

Am I wrong?

MR. BEARD: Well, we are to a certain extent getting ahead of ourselves in the presentation, but to answer your question directly, number one, no one has said this is an abnormal performance yet. What has been proposed by the regional office is either an abnormal occurrence or a Category 3, which are other events of interest. The reason it was considered for an anormal occurrence, because one of the safety functions around the plant is to provide emergency power when you might need it. This plant, this station was for a period of time, albeit 15 to 30 minutes, which may be brief, it was for a period of time with no emergency power. That is the major degradation of an important system to safety. I think it was along those lines that it was considered an abnormal occurrence, but that is not the issue here today. That is not the issue today.

I would prefer to go on to the events so that we can get on to the comments at the end.

MR. EBERSOLE: I think that this brings up a question about should you report the .45 caliber bullet through the hair if it didn't get your scalp? I think you should because I think it is a --

MR. BEARD: For AC owned reactors, when I worked with them, we used to have all the operators report near misses, and we had to try to explain to contractors, somebody like Savannah River DuPont what we meant by a near miss. The example I used to use when I went around to the plants was if Mr. Ray is in his office and he steps out to go to the bathroom, and about that time the ceiling caves in and it covers his desk and all sorts of stuff, it was fortuitous for him, maybe providentialy that he was out of the room, but that's what I call a near miss. He was one step away from it.

And I would agree with you, near misses like this should definitely be reported.

MR. EBERSOLE: Another thing, what this foretells here is there is an absence of a matrix system to do maintenance and surveillance. I know a system proposed a few years ago was a matrix that said no one should work on Relay Pump B and the valve of system C. I think it is probably rampant right now in the field that this sort of a combination of maintenance can sneak up on you, and it just didn't get the last element.

MR. BEARD: Well, I believe that clearly the utility involved -- I guess PG&E would be the first to tell you that in retrospect it probably wasn't their most prudent move to take that transformer out for painting that particular week.

MR. BARANOWSKY: But this is exactly the kind of thing I was talking about catching through tech spec and LCO revisions. They need to be --

MR. EBERSOLE: Matrix.

MR. BEARD: I have a comment on this at the end.

Okay, can we move on to Quad Cities?

Quad Cities, again, is a two out of three set-up with regard to diesels. They had a temporary loss of two of their three diesels and loss of all offsite to one of the two units. The reason this one is important is because it sounds like the one above it. One diesel was out of service for routinew reasons, the start-up transformer for the other unit was taken out of service for routine reasons. The unit tripped. The shared diesel started, and it tripped because of improper adjustment to some of the set points, and the second diesel started and ran, providing power okay.

I might point out that during this event there was a loss of instrumentation in the control room and, like some other events, the operators did not know which events to believe or which not to believe, and they had to send people outside the control room, outside the archways, to find out where the control level was.

San Onofre was a very simple event. Instrument line measuring loophole pressure burst, sprayed lube oil down on hot pipes and, of course, it caught fire. It only involved one diesel. No interaction.

(Slide.)

Okay. Moving right on, emergency tech spec changes. What I would like to do here is just run through these things as quickly as I can and just hit some of the highlights. You will see on the first page there are three Farleys. The major points here are that the first one involved Diesel 1C, as it is called at the plant, which is a Fairbanks-Morse or Colt unit at the 2850 Kw size. This particular unit, it is a shared unit. It will provide power at either unit to what is called Division A.

The problem is they found water in the cylinders and they thought it was an O-ring problem. The important point here is it took 13 days, they estimated, to fix it. They had a three-day or 24-hour CO. They asked for an extension on the plant.

In addition, when this was done, the NRC suggested that while we are giving you something like 13 days, we do not really think it is a good idea to be test-starting every diesel at this station for this period of time. So we changed the action statement testing requirement for a this-time-only basis, that they would check every 72 hours instead of every 8 hours.

There was another event. The same sort of thing happened with the same diesel. This time what they found out was that when they went into it real good the risk pins were gone. That was causing the O-rings to go. They needed ten days to fix it. They needed a 15-day extension. We granted it.

Farley Station involved another diesel, but it was the same manufacturer and the same cause. This time they found water in the heads and they had a little side damage.

(Slide.)

I would point out that at the top of the next page, the last item is crucial under the first event. The NRC requested, after this three times in one summer situation at Farley that even though the plant safety was not in jeopardy we felt like continued tech spec changes were not the best way to go, so we asked the licensee to come in with an overall look at it and come in with some permanent changes, which they did.

At Peach Bottom, one of the diesels failed, Fairbanks-Morse, about the same size. They needed ten days. They had a seven-day LCO. We granted it after ten days.

At Hatch a major failure of Diesel 2C, they call it. This is dedicated. Here we get into a situation. The Hatch plant is one of these where there are two reactor units at the station. Each unit has three emergency busses and it is a two-out-of-three success on a per unit basis.

We had a lot of discussion this morning about what two-out-of-three means. Here is a general exception. This plant does have three sets of emergency busses.

In the Brunswick case we had a failed diesel. It was a Nordberg. The reason this one is interesting is because the station design at Brunswick is the so-called stationizer-energized design Mr. Ebersole brought up this morning. They have four busses, four diesels to provide power to the station overall.

The busses are not unitized, if you will.

They are not dedicated to a particular unit. What you will find is that at Brunswick if you take, for example, the RHR pumps, put one on one bus, one on the other bus, you will find loads for each unit for the same division of power for those busses, and it is very complicated.

(Slide.)

Okay. The significance of this event was that they needed a couple of extra days on the repair item. We in OREB were concerned about the impact on the other diesels at the station and we got a metallurgical report in from the first diesel. What it said was the components that failed were due to fatigue due to excessive starting.

We looked into this. We found out that that particular diesel failed had 1,638 starts in a period of 80 months.

MR. EBERSOLE: Isn't there a requirement like there is on aircraft engines that after a certain number of evolutions of at a given time that you have to go in and replace the part?

MR. BEARD: I have a comment on that very point coming up. The other diesel units at that station varied from -- well, 1,600 was obviously the largest -- from 1,200 on up. It was not something unique to all diesels. They were all high starters.

After they found that out, the NRC made them -- well, the licensee agreed to test inspect the other diesels before they restarted the other units, and they found that -- Doug, was it three of them or four of them had the same disease. It was either all of them or only lack of one.

Hatch, the other problems. Diesel 2C, Fairbanks-Morse, connecting rod failed. The licensee and manufacturer as a team estimated 18 days for repair. They came in for an emergency tech spec change. This one is interesting because one of the questions we raised was, neglecting for the moment for the period of time a major LOCA, a more frequent probability occurrence would be loss of power on the offsite system.

If that should occur, can you bring the plant down? It turns out the answer is no. They could not take a single failure and bring the plant down, even though there were four diesels left, and we will get into this later.

This has relevance in the sense that this morning we were talking about the assumptions that one diesel per reactor unit is sufficient to bring the plant down. This is an example where that is not the case. They require four to five for a LOCA and they require four to five for loss of offsite.

MR. EBERSOLE: How did that escape the regulatory review?

MR. BEARD: May I take the Fifth Amendment?

(Laughter.)

MR. BARANOWSKI: It meets the single failure criterion.

MR. BEARD: Yes, but I would prefer not to go any further.

(Slide.)

Before we go to this, can we go back to that one?

(Slide.)

The tech spec change was not given. The plant shut down, did the repairs, and following the maintenance they tested the diesel. It failed again, wiped out the main bearings and, because of that, the NRC asked them to inspect the other diesels and, again, three out of the four had the same problems.

(Slide.)

Okay. That is as far as we went on emergency tech specs. What I would like to do at this point is give you a summary of some previously-existing information on the types of failures from our perspective with what the industry has shown before the

A-44 study.

There was a report published in '75 that capsulized the experience from '59 to '73 and indicated the major problem was starting. Thirty-five percent of the diesel problems were starting. Other problems, such as the engine, the governor, which I have underlined and will come back to, cooling systems -- there were about 19, or 12 percent each, which is small compared to the 35.

A point to be noted in passing is right after the report was published in '75, in '76 -- in the '75 to '76 area, that was the development area for the issuance of Reg Guide 1.108.

There is another report that covers the experience between '76, '77 and '78 -- a three-year period. The major significance of this one is it indicates starting is no longer the major problem. Problems are pretty uniformly distributed, with the governors, starting and fuel problems all at about 17 to 12 percent each.

I was asked in preparation for this briefing, someone was apparently interested in do we have any obvious bad actors -- you know, one particular vendor, one particular machine, whatnot. That is a tough question to answer. Based on the same '76 through '78 experience reported, it appears there may be one. Okay? I am not saying there is.

Fairbanks-Morse, with the size around 2850 represents 16 percent of the diesels we had at the plants during that period. The reason why I say it might be a problem area is that according to this report these have had more failures per machine, since they amounted to 24 percent of all failures from 16 percent of the population. That may or may not be significantly great.

Secondly, a higher percentage of their failures amount to long repair times. In other words, if it takes over 24 hours to fix it, you might call that a long repair time. What it amounts to is that for that vendor that size, 16 percent of their failures are long repair times, as compared to the average of 10 percent.

Okay, number of test starts. This is not coming out of the '76 thing. Some of our diesels out there we know from experience and talking with the utilities and the manufacturers and whatnot are getting 16 to 18 starts a month. Now there are two reasons for it.

One is that they get on the basis of low reliability test results, they are failing frequently at the last 100 starts. They found a Reg Guide that makes them test them every three days, so they test them every three days.

The second contributor is because they go into the action statement, because they have lost some piece of equipment, which they will sooner or later, they find themselves in an action statement that requires them to be initially started after the first hour and be repeated every eight hours.

In passing, I would like to say that at one of the plants I talked with, if you take the number of starts that they had, it turns out, I think, theirs was 18, you subtract the number required for routine testing, and the number required for post-maintenance testing, and you attribute the rest to LCO action statement testing and say maybe that is 14, 15 starts per month. How long do you have to be in an LCO action statement and degraded mode to get 14 or 15 test starts?

It turns out that that test interval is 12 hours and they are in an action statement about one week a month -- one week a month on the average.

Okay, with all that as background --

MR. LIPINSKI: Before you continue, that 8-hour LCO condition, there is an implication that if that diesel is tested and it successfully starts and runs and you shut it down that you have got some kind of a criteria that says the probability of failure is proportional at time and, therefore, you put the limit on it at 8-hour intervals as opposed to, say, 24?

MR. BEARD: Let me see if I can try to give you a feel for what I am aware of. If you lose, say, one of the diesels at a multi-unit station, you are required to go around and test all the other diesels immediately, within one hour, according to the standard tech specs today. That does something for you.

Then you are required to repeat that every eight hours, generally, I would say, to demonstrate continued reliability.

MR. LIPINSKI: But that is based on an assumption that there is a linear failure rate. Once you start it and run it, you are assuming that there is something that happens to those diesels as a function of time that will prevent them from operating the next time on challenge.

If you have some sort of a reliability target, then I could understand your eight hours, if you have this failure rate number that is proportional with time.

MR. BEARD: I guess the best way I could answer you is a little bit abstract, but I do not think that the basis for Reg Guide 1.108 was that rigorous. I think it had to do with a lot of engineering judgment.

You know, the NRC and the utilities have been trying for a long number of years to get the reliability of the diesels up to a desirable level. We have been making improvements over the years. In '77, when the Reg Guide was issued, they were required for a lot of testing during refueling, like a major test run, three-day LCOs, et cetera, et cetera. It came out with a monumental improvement, which was test frequency based on test failures, which I think was an effort to improve it.

To presume that there was this rigid, rigorous analytical basis for every item that is in the Reg Guide for the standard tech specs I am not certain is always the case.

MR. LIPINSKI: Based on what you have just said with respect to how often they are in the LCO conditions, how often these diesels are being started, would engineering judgment tell you that an 8-hour interval is too short?

MR. BEARD: I have that comment on the next page.

(Slide.)

This is the brunt of what we came down here to say this morning or this afternoon -- general comments that are not necessarily statistically sound in the sense that we have a rigorous basis for them. They are engineering judgments based on having gone through a lot of this experience on a real-time basis and being involved with the emergency tech specs and the basis for those.

The first category has to do with event reporting reliability assessments. That has to do with you should not be simply trying to assess diesel reliability by counting LERs. That will lead you astray very quickly. I think the people that Baranowski had working for him have done a commendable job in reviewing the categories and categorizing them in what I would call the real failures, where a diesel would not work when you wanted it, not that it would not work when you tested it and so forth.

The second point, and this is one of the major comments, is that even though the average reliability may be satisfactory, the extremes are significant, as we have discussed earlier. I would point out at this time that it is my understanding of the way the calculations were presented this morning that those are not plant-specific numbers either, to the extent that they took a plant-specific fault tree -- and it is my understanding they used national average failure rates.

I will stand corrected. I will stand corrected. I misunderstood you on that.

For overall global approaches like the mission they make for generic requirements, you have to use average inputs, but the extremes are very big. That is the point I wanted to make.

All right -- shared systems. Let me hit the biggies here. Most events are with shared systems. The big thing here is that in the second item often a shared system multi-unit station can take single failure on the station, but not necessarily single failure on a per-plant basis. So when one does go down, you may be in trouble.

MR. EBERSOLE: May I make a comment on that? The reason for that is the purpose of sharing was to reduce cost and make the single event per station instead of per unit. If you, on the other hand, had a criterion for a single failure per unit, and then took the resources available at a multi-unit plant and redesign them on an integral base, you would have combined multiple failures per unit.

Do you follow me? I am saying do not dilute the plan by sharing it. Rather, reorganize it to make available multiple failures per unit.

MR. BEARD: Well, I think, with all due

respect, sir, the bottom line, in my personal view is you end up with a two-unit station with only three diesels.

MR. EBERSOLE: No. I am saying if you wound up with four instead of two, if you organized them into an integral plant design you would have a better rig.

MR. BEARD: That is what Brunswick did on a per-station basis.

MR. EBERSOLE: Did that not give them the prerogative of two failures per unit? If not, then it is a failure.

MR. BEARD: I think it does give them some additional flexibility, but there is another comment coming up that may be a drawback to that.

MR. EBERSOLE: That is the price you pay for complexity.

MR. BEARD: I think it comes back. I do not want to be simplistic about this, but my mother used to tell me you do not very often get something for nothing.

MR. EBERSOLE: Never, in fact.

MR. BEARD: One of the problems we are observing is, any time you do have shared diesels and that diesel develops a problem, the tech specs come into play, and you are in a situation where legally both plants may be asked to come down. Now, there is a tremendous impact economically if you are talking about bringing 2,000 megawatt units down to the ground.

MR. EBERSOLE: Right. On the other hand, if you were on a unified basis, you would have to have one unit down whereas if you were on an integral basis, you might have the flexibility to maintain both units in operation. So there are two sides to this coin every time. I think you simply have to weigh both of them.

MR. BEARD: True. Another significant comment I had is that the assignment of support systems such as not the RHR's but the RHR service water to the emergency bus may in some cases be crucial and limiting. The example I gave here is, there is at least one two-unit station that requires the diesels to come down from loss of power without any reactor transient, let alone an accident. That is because of the distribution of the service water systems.

The last comment I had has to do with an integral approach or a system design approach where you have four diesels that provide power to the station as a whole. The problem you run into here is the loss of any one station affects the loss of both diesels. They are both reactor units, and it is complicated to analyze, because you do not have a unitized approach in the design phase. You only have a unitized approach in the tech spec phase.

(Slide.)

MR. BEARD: Testing requirements. Here is where we might get some discussion. Our operating experience seems to be telling us that the requirement for testing, test starting the diesels on a routine basis -- by that I mean, when you have no failures that you know of -- on a three-day basis ought to be reconsidered. There have been cases where it has contributed to failures, and we have cited one or two of those.

When Reg. Guide 1.108 was developed, I believe it was believed that no one really knew the optimum test frequency. It was set up in a monumental way as a big step forward, somewhere between three and 31 days. It looks like possibly now 14 and seven-day test intervals are the best options.

The second item here is testing ought to have as an explicit purpose to identify "unreliable EDG's," diesel generators. When I wrote the word in here, I had the term "lemons." The term was not acceptable. All right. My management suggested to me that maybe for a presentation in front of such a noble group as this that we should not use the term "identifying lemons."

MR. EPLER: Oh, yes.

MR. RAY: Maybe sour apples would be better.

MR. BEARD: It came out "unreliable diesel generators." When you do identify an unreliable diesel generator such as one that has had 12 failures in 18 months, we believe that major corrective action ought to be taken, not just tested more.

MR. EPLER: That's right.

MR. BEARD: But that is what the NRC instructions say to do. Okay. We believe also that our experience seems to be telling us that test frequencies during the action statements which have been brought up a couple of times should be relaxed. We think there are two primary purposes. One is, when you have a known diesel failure, you want to make sure the diesels are not going to die from the same disease, so you test them fairly promptly to determine they don't have that same problem. But I think the commotion that is created in the first hour following that event, you probably ought to do it promptly, but not necessarily in one hour. Maybe four to eight hours might be more appropriate.

Secondly, we think testing them every eight hours repeatedly after that might not be the best thing. In other words, we have learned more from our operating experience. My suggestion or our branch's suggestion, and we are talking with the other sides of NRR about this, is to see if it wouldn't be more appropriate to go with something like 48 to 72 hours, some number in there.

Another item in here had to do with Mr. Ebersole's comment earlier about manufacturer's recommendations after some interval of time. You have to tear it down and look at it. We think you should do that. We think after so many starts and or so many hours or months of operation, whatever, the diesel ought to be torn down so that you can find out what is wrong in the inside. Test starting won't tell you about anything wrong on the inside until it dies. We have had enough experience with common situations that I think it is now time to start thinking about that.

MR. EBERSOLE: Well, of course, that is mandatory on aviation engines, and I am not so sure but what it isn't entirely appropriate that it should be a mandated regulatory requirement here. I am suggesting that.

MR. SAVIO: Do the manufacturers have that type of information? I looked through the list of LER's that Oak Ridge provided at this Brunswick one on the failures that I found that look like they were due to the fast start. It appeared that there were things that just were not discovered until the pieces were on the floor, so to speak. The Brunswick case in particular was a shaft which seemed like a fairly simple configuration, something that could have been evaluated beforehand.

MR. BEARD: Yes. I think -- Doug, help me with some of the details. The down pins were sheered and the couplings came loose. What happened was, when they looked at the other diesels and took them apart, they found that there was the same situation. They hadn't already broken in the other diesel.

MR. SAVIO: They found the first one.

MR. BEARD: But with all due respect, I would say that those diesels would not have been inspected prior to starting both of those units back up if the NRC had not stepped in.

MR. EBERSOLE: May I suggest that you look into the matter of noise analysis? And I don't mean neutron noise, I mean physical noise, by transmitting equipment on various places on the crank case and so forth. These things have an interesting signature which is individualized, and a departure from the normal signature which can be put on the scope or the trace and even examined for frequency bands or whatever. I think it would tell a lot about whether you are borderline to failure.

Generally, people go down and say, listen to it. It is running like a sewing machine, or it is about to disintegrate, but that can be done somewhat more methodically than that.

MR. BEARD: That is true. I try to convince my wife to do the same thing about the car.

MR. RAY: This area of testing requirements, Mr. Beard, opens a subject which concerns some of us, and Mr. Epler in his comments earlier this afternoon touched on it. Apparently, the frequency of starting required has a mechanical stress on a unit. It causes damage and so on. The testing requirements that require a fast start, the point that Mr. Epler touched on has been pointed out to us by one of the ACRS Fellows, Mr. Richter, who is here today, suggesting that possibly eliminating the requirement of a fast start on tests would not -- memorizing the number of such starts might very well maintain the diesel generators in a better state of health and therefore in a better state of reliability. Has this ever been considered by the staff?

MR. BEARD: I think the answer to your direct question is, I am sure that it has. I personally was not involved with it, however, but I think the idea that your Fellow has suggested probably has merit. Our experience indicates that you probably would not want to reduce the number of fast starts to zero, but maybe do it on a quarterly basis. Certainly in my view if your purpose of starting a diesel is to do a 24-hour test run, you don't have to fast start at the beginning.

MR. RAY: And if your purpose is to indicate readiness to serve, you need not have every test a fast response test, but periodically have such.

MR. BEARD: There is a lot of merit in that.

MR. RAY: Later this afternoon I hope we have time enough for Mr. Richter to give a brief presentation of the considerations he has brought to bear on this phenomenon, and that maybe out of this we might precipitate staff consideration of the thought. Yes?

MR. EPLER: Mr. Chairman, I think I recognize the need here. Fifteen years ago John Anderson, who sits right there, and I collaborated on a paper on testing, what is it, what do you expect. One of the things you expect to do is to test it to see what the designer expects it to do. You do that once, if you can. You can't test a double ended large break LOCA. You have to take that on faith. But you can test some of the other things.

Another thing you do is to test routinely to see if it works today like it did yesterday. That is, have there been any component failures. Now, why are we testing diesels to detect what? If you test it once to see if it is capable of fast start, if no component has failed, shouldn't it continue to fast start? We need to define more carefully why we test, I think.

MR. BEARD: With all due respect, sir, being a follower of your work for many years, I think that one of the purposes that you do testing, be it on diesels or one out of four instruments on HPCI or whatever, is because we have adopted a two-train approach, which means we can take a single failure. Therefore, we test frequently enough to see that we find a single failure before it is a double failure. So, that is one of the considerations.

MR. LIPINSKI: I would like to go back to your second bullet up there in the Reg. Guide. Given that a diesel has been tested and possibly has a failure to start or starts and has a failure to run, I assume a diagnosis is done and a correction is made before the next test is conducted, and your second bullet up there kind of implies that diagnosis and corrective action is not taken if you have a failure to start or a failure to run.

Now, if a program is being conducted properly and you are trying to demonstrate reliability, if you do have a problem, I assume that problem is diagnosed and corrected before you try to go ahead and start the unit again. Now, what is the experience in industry with respect to trying to demonstrate reliability via the Reg. Guide?

MR. BEARD: I don't want to imply, sir, that the utilities are not when they experience a failure trying to find out what caused it and fix it in a very prompt sort of way. I don't mean to imply that at all. I guess what I am trying to say is, if you go back to one of the events we discussed a little earlier in the presentation, I believe it was addressed, where they had a flow blockage that was due to air binding. When it happened a second time, they looked into it very much further, and they found out the check valves were messed up and that was what was causing the flow blockage.

MR. LIPINSKI: That gets into the diagnosis problem.

MR. BEARD: I guess you get into the classic situation. You have a utility that makes money by putting watts out on the line. They want to get the diesels back up. They want to get whatever equipment back up, give it a reasonable time for diagnosis and repair, but they are not trying to make a research project out of it, and you have this dichotomy we have seen for years, the goals and objectives of the safety people competing with the goals and objectives of the production people.

I guess what I am suggesting with this comment up here is that when regulatory requirements are revised as we are continuing to do from time to time, it might be a good idea to put in there some requirements that if you have a machine which repeatedly is having major problems, you ought to look at it not from the point of view of merely testing it more often to show something. Testing in my personal view does not make a machine more reliable. At best, it can only increase your confidence in what you think the reliability is.

MR. LIPINSKI: But that goes back to my original observation. The tests will not verify the machine. If you have trouble, you have to diagnose and correct the problem. Are you going to be able to regulate that diagnosis be done correctly?

MR. BEARD: Mr. Srinivasan is here.

MR. SRINIVASAN: Srinivasan, NRR.

Your point is a good one. If you look at the Dayton study, one of the fundamental conclusions of that is, they do have a maintenance program, but they are not being implemented adequately, especially on those diesels which have seen more than the average number of failures. What the staff is currently doing is, with regard to the recommendations, it is trying to go back to the area of reactors who do not have a severe test frequently like the NTOL's have, and look at their maintenance program, look at their operator training capabilities, how well they are trained.

We have a lot of real experience -- Brown's Ferry is one, Zion is the other -- where at the initial stage they have a number of failures. They have tested frequently. Ultimately they have found out there is nothing wrong with the machines, but the machines have not been adequately maintained. Good housekeeping practices have not been followed. And that is the lesson we learned. One good lesson we learned from the Dayton study is upkeep of the machine.

Our current program is to go back to some of the older reactors and look at their maintenance program more rigorously, and see whether they contribute to some of the failures. Testing alone will not cure this. Prior to testing, once you have testing, you have failure. Before you conduct the next test, one has to determine what caused the failure in the first place.

MR. LIPINSKI: But there is an assumption that you diagnose correctly, and as we have seen in some of these, they have had a first guess, thought they had it fixed, and then found out they didn't fix the original problem. Do you have anything in your program that will help proper diagnosis based on past experience?

MR. SRINIVASAN: What we intend to do in some cases, the failure of such a nature, they haven't been doing good analysis of the root causes. They have been sort of a bandaid fix, and try to go on to the next unit, and they come back to this unit the next month and it fails. The program we are currently putting together is to give them a much longer time than we now have in the tech spec. That will be an incentive to the licensees to do a better job of assessing what is the root cause failure of the set before they move to the next testing cycle.

I hope that answers your earlier question.

MR. LIPINSKI: We are doing a lot with symptom emergency procedures in plants. You should do the same with diesel generators.

MR. BARANOWSKY: I think you need both the carrot and the stick approach. In other words, you can't just say, I will give you longer LCO's, and you will be good about it and fix the machine up. You need to answer the same thing. If you don't fix it, can you run your plant with an unqualified diesel generator? So there has to be some sort of a punitive situation in there. A $5,000 fine won't do it. It has to be a reasonable type of procedure such that you are not causing everyone to shut down every day for undue reasons.

That is the kind of stuff we would like to look into in terms of looking into future diesel generator reliability. The aspect of Reg. Guide 1.108 was, you test the machines so often until you break it. That was the punishment. Maybe that is the wrong kind of punishment. I don't think you can mandate that people have great diagnostics. They have to want to do it. If they refuse to find out what is wrong with their machine and make replacements when necessary, then you have to look at, is that machine qualified to be a safety feature. If it is not qualified, then they don't have that division. Can they operate the plant with one division in that case? I don't think so.

MR. BEARD: Let me say also, having been involved with a number of emergency tech spec requests, the utilities are trying to find out what is wrong with these machines. There is no doubt about it. In fact, I would venture to guess, my own personal experience, when I take my car in to get it repaired, when I take my TV set in to get it repaired, or when I call a plumber, I would rather have these utilities chasing down what they think is wrong with their diesels because they do a hell of a fine job. That is not the essence up here at all.

I think we are digressing more into a general discussion. Why don't I get these last two points, and then we can get the slides out of the way.

The last point had to do with the events we talked about before. Licensees really ought to be quite careful, if not warned about taking off-site circuits out of service when the diesels are already out of service, one or more of them, especially when there are routine reasons it could easily be delayed for a week. I remember experiences about containment entries not too long after TMI. One of the requirements was, don't go into containment just because the Vice President's son wants to have a tour, and I am suggesting the same kind of approach.

MR. EBERSOLE: You have made that applicable here to the diesel generator problem, but that is a generic problem. That would be applicable to service water component cooling, whatever, and yet it is not.

What it really means in the broader context, I think we should invoke a matrix system for disabling and repairing equipment. That was proposed in 1968 by GE and NRC threw it out the window and went to this arbitrary thing without any consideration about cross flow of influence and the non-presence of a matrix. That is 20 years ago, more. I think its time is due again.

MR. BEARD: Maybe it is.

MR. BARANOWSKY: Absolutely. We have recognized this in the reliability and risk analysis field, and what we want to do as a research program over the next year is look at this kind of a matrix approach, not only identifying what things shouldn't be taken out at the same time, but in identifying what should be the outage time.

What you have now is a set of LCO's that are primarily based on judgment or the perceived risk associated with taking a certain component out. It would be a lot better if we don't take and make an LCO on a diesel generator three days when for all other failure reasons caused by trying to make repairs within three days, our unreliability is so great that we haven't achieved anything through an LCO.

MR. EBERSOLE: Pat, your observation about time, I have always had trouble with time with respect to its real meaning concerning progressive degradation. Time is merely a vehicle of sorts that carries a chain of events. A long time with zero events is no time at all, in the context of what we are trying to get at, and something with significant events in that interval is another thing. Time is kind of a universal recognized symbol for doing these periodic tests, but I think we have to look at time in the context that I am talking about. It is the sequential flow of things that happen in time that either degrade or permit the engines or equipment for that matter. It is this angle to be changed. I think we ought to look at time on a qualified basis.

MR. BEARD: The last comment I had was that when major failures occur on a diesel machine, being a big mechanical device, the present requirements of three-days outage or shut the plant down or even the seven-day outage or shut the plant down do not hack it in a lot of cases. Hence we get a lot of requests that say, can we change requirements temporarily once in a while.

MR. EBERSOLE: Again, the days don't mean anything. It is the succession.

MR. BEARD: Well, there are a lot of people, sir, who believe that we can associate a number like three days, 90 hours, with some figure like 10^{-2}. That is an exposure period. The probability of something happening to you. It is a risk figure. And they use these things, and I think there is some merit to their use, but we can't get locked into where everything is a number.

MR. EBERSOLE: But in the matrix context, it would have to be associated with what is happening in the interim.

MR. BEARD: Absolutely. Let me say in summary what I have tried to do today. We have tried to tell you that we are not coming from a background of analyzing a bunch of LER's, questionnaires, or whatever, although that is good, and I think the people with Oak Ridge and Sandia and under Pat's direction have done an outstanding job on it. We are coming to you dealing with operating events as they have occurred, if you will, and we have tried to present to you some of those events. We have tried to present to you some of the emergency tech specs we have been involved with, and tell you what our experience seems to be telling us.

I would caution that we put everything in the context that Power Systems Branch, NRR, I&E, the industry, we have all been trying to make these diesels right, and we are learning more every year, and these are just our judgments on recent experience.

MR. EBERSOLE: May I ask something about the nature of tests? It has bothered me to see tests be of a sort of bi-stable type, for instance, with valves. If it opens and shuts in a proper time interval, it passes the test. The fact that it did it with the last inch of torque and groaning, screaming and smoke does not reflect whether it was a successful test or not.

When you test the diesel, is it implicit that somebody goes down and looks at the exhaust and sees whether there is smoke coming out of the generator or not? Or oil all over the floor? Is it a comprehensive test by people who know diesels?

MR. BEARD: Clearly, that is the intent of the regulatory requirements that people test it the way things ought to be tested. Clearly, there is also the incentive on the part of the utilities to test it as best as you can, because they know if they can detect early failures, early wear, a little smoke coming out of the exhaust, just like your car, sooner or later you know you are going to have to take it into the shop and fix it. The problem is that with utilities or the situation with utilities, it is that they know when that goes down it is going to cost them $750,000 a day outage time. So, there is clearly an incentive for them to test it right.

My only observation I can give you is, I have not been in a control room any time when valves were tested, but I have been in there some time and valves were required to close in five seconds, to demonstrate that, Number One, they would close, and Number Two, at an appropriate time. The tests were conducted with the guy's wristwatch who is in the control room. He pushed the close button, he watched it with his wristwatch. Sure enough, it closed in 4.65 seconds.

Now, that is the way some testing is done.

MR. EBERSOLE: But it is not mandatory, I guess. It is just thought to be in the best interests of the utility, therefore they will do it.

MR. LIPINSKI: Getting back to your comment on the three-day or seven-day LCO covered repair time, how do you propose setting a repair time? Where 50 percent would pass?

MR. BEARD: We are having to do that currently on a case by case basis right now. It requires considerable review on the staff's part to see how much is safe and how much is not. You can see one of the tech spec requests I had on the cartoons was actually withdrawn after we looked at it. We are looking forward to the program that the Division of Safety Technology has proposed now. We think it is a very well thought out, comprehensive program of clear safety goals that we understand is going to be described in a few minutes.

Basically, the part that we like is, you don't give them three days, paste it back together, start it, and take it back for another three days of repair and maintenance. You give them a period of time scheduled over a year, and you say, you can take it all in January, or you can spread it around, keep it in a little reserve. But when that day comes, the plant comes down.

MR. LIPINSKI: Maybe I am misunderstanding. I am assuming I have a two-diesel station and one diesel is a failure. You are going to allow that plant to run with one diesel for a year?

MR. BEARD: I am sorry. What I am saying is, rather than giving them a per-outage limit, the proposed program from DST, as I understand it, would give them a cumulative number of days the diesel could be out per year. For example, if the remaining diesels are the highest grade of reliability, one diesel could be out for maybe 28 to 30 days a year. If the reliability on the other hand of the remaining diesels is four, you may only give them five days in the year.

On the other hand, if the reliability is very low, you say, look, if that diesel fails, the plant has to come down. But by giving them the flexibility, we are curing some ills, making it better, and giving them -- you know, if they do have a major outage and it takes 14 days to fix it, they have got the time to do it with.

MR. LIPINSKI: Does it follow necessarily that if I have a bad diesel, that the other one is going to be of superior performance? Usually when we see one name pop up there, the other diesel is having the same trouble, if it is by the same manufacturer.

MR. BEARD: There are some people who feel like, say, because all of Brand X, Size Y's are giving troubles, you ought to get rid of them, or do something drastic. On the other hand, I think the experience is, you may get one limit in that size and it is a maintenance hog, if you will. In that case, you may have to do something drastic, but I think it might be stretching the statistics a little bit to say all of a given type are bad actors just because a few are.

MR. LIPINSKI: But looking at the specific plant data you had up there, it looked like if one was bad, the others were bad.

MR. BEARD: It turns out at that particular plant I think you are referring to, the utilities would love to have a different type.

MR. RAY: Does that terminate your remarks for the day, Mr. Beard?

MR. BEARD: Please.

(General laughter.)

MR. RAY: Fine. I assume there are no further questions. I would like to declare a ten-minute break, and I would exhort those of you who are sitting here today now to come back, because we would like to get across to particularly the NRC representatives the thoughts that Mr. Ryder, Chris Ryder of the ACRS Fellows staff has developed, in the hopes that through some channel you might indicate we can communicate it to the staff. So, we will resume the meeting at 4:00 o'clock.

(Whereupon, a brief recess was taken.)

MR. RAY: May we resume the meeting, please?

I would like at this time to call on Chris Ryder of the ACRS Fellows Group who has some viewpoints on test starting of diesel generators that I would like very much to have considered by way of suggestion by the Staff in considering regulatory requirements in the future for such things.

MR. RYDER: Over the past several months I have been looking into improving diesel generator reliability and getting power to the emergency systems when they are needed, and I saw that one of the ways to go about this might be to modify the startup requirements.

(Slide.)

MR. RYDER: After thinking about it a while, I came to the conclusion that the capability to do -- to perform the emergency functions is really a combination of both reliabiity and operating procedures.

(Slide.)

MR. RYDER: Here is some like overall reliability estimates. Although they are not too bad, they are usually around 98, 97 percent, there is always a certain amount of unreliability that we are always going to have to deal with, and I think like no matter what we do to the engine, we can put one improvement on after the other. There is always going to be some small amount of unreliability that is going to be around and we are going to have to be concerned with.

MR. LIPINSKI: Before you take that off, is there a digit missing behind that nine in the last column?. You have a 9 percent confidence interval.

MR. RYDER: Yes, it should be 95.

(Slide.)

MR. RYDER: One of the problems with diesel engines is really the way we use them. We do the wort thing you can do to an engine, which is start it rapidly from a cold start. I don't think like any of us would start our car in January from a cold start and get down the block and have it at 60 miles an hour unless you want to go around the block and pick up the pistons on the way back.

The manufacturer has said that rapid starting causes large dynamic forces in the engine. It causes insufficient lubricating oil to the components. It causes insufficient air to burn fuel, which leads to exploding fuel and burning of the lubricating oil and piston walls, and it also causes the components to heat up in a heterogeneous manner and causes excessive engine wear.

Some utilities have gone to addressing these problems by going to a smaller engine, but still the problems exist. The San Onofre units on Units 2 and 3, are getting, instead of one large diesel engine, they are getting two smaller ones to drive one generator. But still they have the problems with rapid starting.

MR. LIPINSKI: Have any of the LERs reflected engine failures as a result of rapid engine starting?

MR. RYDER: It is sort of dsifficulty to identify. I guess what the manufacturers are saying is more like an intuitive thing. It is obviously not good for the engine but we don't know exactly like how it is being reflected in failure data or anything like that. It causes a lot of stress in engine components. It causes the components to wear, either because they don't have oil or because they don't have -- they are expanding at different rates and things like that.

MR. LIPINSKI: That would be true, but then I might need 1000 or 10,000 of these incidents to cause final damage. In other words, one event is not going to destroy the engine. Otherwise you would say I have an LER that is associated with the rapid start. But out of all the tests that have been run on specific engines, if there isn't a specific LER, then the question is what does this contribute to engine failure?

MR. RYDER: You will see in a little while that there will be -- there are several ways of addressing the procedures.

MR. BEARD: May I remind you that in the presentation I made we have had a couple of experiences where the failure of diesels was directly attributable to excessive starts? So there is at this point in time some documentation of what a number of us have felt over the years intuitively, that if you start them too much you are going to wear them out. So I can't give you the direct answer of what LER it is, but there is the experience.

MR. LIPINSKI: The excessive starts number how many?

MR. BEARD: Well, when the diesel at Brunswick failed, it had 1638 starts on it. The vendor at that time said one of the lowest number of starts at that station was 1200, so the inspection point says 1000 though he said 1200. Then they found 1200 failed or were on the verge of failing, so he changed that to 1000. So I can't give you a hard and fast number, but I would say it is something probably on the low side of 1000.

MR. RAY: Mr. Beard, these failures involved mechanical failures?

MR. BEARD: Yes, sir, internal mechanical damage.

MR. EBERSOLE: Compression is all starts now, excessive starts. That is, they are scratch outs. They are full blast, full bore starts.

MR. RYDER: Yes.

MR. EBERSOLE: What I think is the answer to your question is the damage doesn't appear as a fast start failure. It is cumulative in character, and finally the engine will just fail in having experienced accumulation from fast starts, whereas if it had a controlled start under slow, warm-up conditions with a lot of supervision, it wouldn't have all the cumulative damage.

MR. RYDER: Correct.

Well to give you a little preview, one and two fast starts here and there isn't going to ruin the engine. It is just the repeated hammering which eventually causes a lot of damage.

(Slide.)

MR. MAC EVOY: There was just a failure of cooling water pump shaft as a result of excessive starts according to the manufacturer. I can't remember the name of the plant.

MR. SAVIO: Brunswick.

MR. MAC EVOY: It was just starting the diesel too rapidly that heated up the shaft.

MR. RYDER: There are several things we could do to improve the diesel generator system. Some of them we have been talking about today so far. One would be to modify the equipment, and we could do such things as put lubricant, circulate lubricating oil all the time under pressure so that the bearings and things like that are not rubbing metal on metal when they first start up. We could maybe change some of the maintenance procedures and make sure the people are maintaining the equipment properly. We may require several smaller engines instead of one larger one. And as I said, like San Onofre Units 2 and 3 are doing that, or we could also change the operating procedures, which is what O am focusing on here.

MR. EBERSOLE: There has to be an inhibit on the circulating, lubricating components. You are inviting liquid lock due to drainage and filling of the combustion spaces because of the presence of lube oil.

MR. MAC EVOY: You also fill up the exhaust manifolds and have a fire.

MR. EBERSOLE: Yes, and have a fire when you do start.

MR. RYDER: I think we would like to change the operating procedures to reflect some of the characteristics of the engine. We would like to maybe recognize an inherent level of unreliability. We would also like to recognize the fact that rapid startups cause engine wear. We would like to have a well-defined purpose for testing. We would like to know either are we going to test it to verify that everything works, or are we going to start it up rapidly to see if in fact it can do that? And it is also interesting to note that standby power is really needed immediately. At least, that is within our experience so far, so that we might start considering some of these when we make regulations and decide how we are going to use the diesel generator systems.

(Slide.)

MR. BEARD: Could I ask a question about that last statement, that standby power is rarely needed immediately on demand? There was a situation where one plant in the midwest had trouble, and diesels would only start in something like 30 seconds instead of the required 10 seconds. It is my understanding that GE did some analysis and determined that had an accident occurred with the plant at full power, that it would have led to a significant amount of fuel damage on a 30 second start.

It is my contention that in spite of the fact the utility got a big fine out of it, that we ought to take the lesson that manual recovery of failed diesels, even if it doesn't start just one time and you push it and it does start, operator response of 30 seconds or 60 seconds is too slow in that it leads to fuel damage. I have reservations about the kind of comments that you had in your last one there.

MR. EBERSOLE: On the other hand, if you are talking about a large LOCA, which I think you are, the coincidence for large LOCA and grid failure is a rather low number.

MR. RYDER: I think a lot of these, like rapid start-up procedures, came out of the fact of the large break LOCA analysis and concurrent with loss of offsite power, but it is my understanding -- and I could be wrong on some of this, but if you have just a plain loss of offsite power, the plant can ride it out for about an hour before you have to start worrying about it, and it assumes, too, that you can monitor the status of the plant all the time and make sure nothing else is happening.

MR. EBERSOLE: What is the nominal number for a large LOCA plus an average offsite power failure?

MR. BARANOWSKY: About less than 10^{-5} per reactor year.

MR. EBERSOLE: Both of them?

MR. BARANOWSKY: Both coincident.

MR. EBERSOLE: Large LOCA plus an offsite power failure.

MR. BARANOWSKY: Yes.

MR. RYDER: But I guess what I'm saying, if you can buy some of that time to make sure that the diesels will start, fine, and if you feel that the plant is in jeopardy, then you can override the slow start and go right into a crash start.

MR. EBERSOLE: That is one of the cases where you don't think about earthquakes, okay, so that is a good number.

MR. DAVIS: Excuse me. I think it would be quite a bit less than 10^{-5} wouldn't it, Pat? The WASH-1400 number for large break LOCA is 10^{-4} and also they used a loss of offsite power of 10^{-3} caused by loss of the plant which would occur during the Loca. So you are talking 10^{-7}.

MR. BARANOWSKY: I said less than 10^{-5}, the reason being that there are some plants that would be more prone to losing the grid if they went out of service, and it could be much less than on the average.

MR. RAY: For a specific plant.

MR. BARANOWSKY: Yes. I just picked out a case that I knew was about the worst. So it is certainly better than 10^{-5}.

MR. EBERSOLE: Here is a case where with a big grid like Florida Power and Light, it would make a big difference as to whether you ought to get a finew or not.

MR. BARANOWSKY: Except that Florida Power and Light has done quite a few things to fix up their grid over the last several years, and you haven't seen the big --

MR. EBERSOLE: Maybe so.

MR. DAVIS: I think we also need to recognize that these LOCA calculations are done against Appendix K requirements, and I don't think that is realistic at all. You can't have any blowdown cooling, you can't go back into CHF. All these things tend to drive that fuel temperature up very quickly, and I think there is plenty of evidence to show that that is not going to happen.

MR. RYDER: I guess what you will see is that the issue is not to ban fast start-ups altogether. The issue is to let's cut them down a little and let's see how we can do that.

During testing it seems likely that we could have frequent slow start-ups just to see that the diesel generator in fact runs, that there is no water in the cylinders and that it is mechanically together. We could do a few occasional rapid starts just to make sure that it can rapid start.

(Slide.)

MR. RYDER: Considering that like testing puts most of the wear on these things, it would seem that even if you did a rapid startup after every fifth test, you have made like a substantial improvement on treating the engines a lot better. But you can also use slow start-ups on demand, too. As I said before, like during a loss of offsite power, you can maintain the reactor for about an hour without having the diesels available, but then after that you really should think about what you are going to be doing quickly. During that time you could slow start, you could inspect, but the problem here now is it assumes that whatever you find you can fix. Now, maybe there are some quick things that you can do to make sure that the diesel will, in fact, start when you need it, and you can go through this idle, warming up and then get it going.

MR. EBERSOLE: May I comment on that statement? That reflects a thesis which is defended by the Applicants that is said to be a case in point, but I dare you to find one who will invite that condition. Any time you suggest it, they run off promptly into a number of reasons why they don't want to do that. I think you will find it very difficult to in real life find that acceptable condition for any length of time. It is a theorized condition, but it is not proved in fact, okay? There are no tests that confirm it.

MR. RAY: Would this apply, Jesse, to a situation where you delay startup for several minutes rather than an hour?

MR. RYDER: We are talking maybe an hour or a half hour.

MR. RAY: But do you need an hour and a half?

MR. RYDER: I guess they are just using that as a figure.

MR. EBERSOLE: Well, seal damage will begin to be at least a thing to worry about. Some overheating will start. One starts moving toward an unsafe condition, and I know, you know, the synthesized experiments that were done at Sequoyah steadfastly avoided any true loss of power. The circuits were backwired to provide a number of auxiliary services which were never denied power during the so-called offsite power test.

MR. RYDER: I guess the point, though, is that you don't need standpoint power in 30 seconds.

MR. EBERSOLE: No.

MR. RYDER: I'm certainly not qualified to say an hour or a half hour or anything like that, but I can say, I think, pretty well that given that nothing else is happening in the plant, you could have a few minutes to at least warm the diesel up and get some lube oil onto the components before you crash it.

MR. EBERSOLE: It might be a good test of confidence in the operators and the applicants to ask them would they be willing to delay the startup of the diesels for 15 minutes and see what sort of response you got.

MR. RYDER: Anyway, moving along, there are some type of demands, too, that you can anticipate. At the distribution centers, the distributors know that they have many half-grid problems, and there is no reason why they can't alert the plants that they are having some problems. In that case there is no reason why the diesels couldn't be started to anticipate losing offsite power because of the collapse of a portion of the grid.

You can also see a storm coming towards the plant, like a lightning storm or something like that, tht might open breakers, and in that case, too, you can start the diesels slowly and get them ready for a lightning strike on the breakers. If it doesn't happen, then you have a test of the diesels. If it does, you are ready for it.

MR. BEARD: Excuse me. Are you proposing that if a utility is operating a plant and there is a lightning storm coming in X number of miles away, that they start the diesels?

MR. RYDER: They could.

MR. BEARD: What would you have them do with the diesels during the time before the storm hits the area?

MR. RYDER: They could just -- what I am saying is they could get them started and warm them up.

MR. BEARD: Are you suggesting idling?

MR. RYDER: I think you ought to reconsider that, and I further would suggest that putting them on the grid as we do in test modes subjects them to any external perturbation than wiping out both diesels. So I think you had better reconsider some of those options.

MR. BEARD: I guess again my point is that it is another situation were there is a pretty good chance that you will need the diesel, so there is no need to crash start it.

MR. RAY: I would like to comment similarly to Mr. Beard's, Chris, on grid collapse, believe me, I know from experience that when they go, they go, and they go in relay time, not minutes, and when transmission lines begin to cascade, they really ding, ding, ding, ding, and they are gone, you are down.

MR. RYDER: In some of the work I have been looking at, not meaning to contradict you or anything, but the --

MR. RAY: Yo are talking about partial interruptions. I am talking about a grid collapse, the whole interconnection.

MR. RYDER: For some of the grid problems, the distributors are trying to like keep the grip up. They are causing brownouts, they are rolling a blackout over --

MR. RAY: That's not a grid problem, that's a capacity problem and they can schedule the brownouts.

Do you understand what I mean? I am talking about transient failures, stability failure of the interconnection. That is very, very, very rapid, and you can't control it by switching.

One way that it can be done -- and it is being done, but then the grid doesn't go down -- that is to anticipate load shedding by underfrequency relays. There you don't lose the grid. Thewy drop load off. They keep the transmission off of it -- on it, and it doesn't affect the plant.

MR. BEARD: I would suggest also that a lot of the reason the plants lose offsite power is not for offsite reasons, it is not the switch. It is the dadgummed startup transformer. They have got protective relays in them that go with the drop of a hat, and when one of those things goes, there is no anticipation of it.

So I think that the intent you have is well-founded, but I'm not sure that some of the premises are very practical.

MR. RAY: You shouldn't be discouraged by your basic suggestion. I think it is a good one and it merits consideration by the staff in my opinion.

MR. EBERSOLE: Well, there are loads available to the diesel if you disconnect the 1E buses connected to that diesel and transfer the safety loads and then go ahead and run a test on them in this interval when the tornadoes are marching around your plant. You can keep them loaded to a point where fouling of the engine would not occur. It will just take a piece of doing, and it is a bigger test than jusdt starting and idling the engine.

MR. BATTLE: If you idle a diesel say at 200 or 300 rpm rather than going full speed, you can leave it unloaded for a long time. Trains, for example, will park and idle for hours. If you are talking about nuclear plants right now, we run them up to full speed immediately, but if you are talking about just a couple of hundred rpm, you don't have to load them.

MR. EBERSOLE: Do they not get oil fouled in the exhaust?

MR. BATTLE: No, not at slow speed.

MR. EBERSOLE: Not at slow speed if you hold the rpm down.

MR. BATTLE: That's right.

MR. RYDER: Also, the final point, the switchyard activities that accidentally opened the breakers can be anticipated and you can start the diesels up then, too.

So I guess the whole point of this whole discussion here is that there is really very little need to crash start the diesels, and yet that's what we seem to do all the time, and there are a lot of situations where we can take advantage of where we could reduce the wear on the diesels and possibly even live with a little bit of unreliability.

(Slide.)

MR. RYDER: So anyway, I recommend that we modify the diesel generator startup requirements to include slow startups.

MR. RAY: I think his suggestion has tremendous merit. My problem, Pat, and Mr. Beard, is how can it be conveyed? How might it best be conveyed by your suggestion to receive serious consideration by the staff? Would you carry it? Is that enough?

MR. BEARD: With all due respect, sir, I think the most effective means for the ACRS to convey a message to the Staff is to write a letter and sign it ACRS.

MR. RAY: Okay, I hear you.

MR. EBERSOLE: Let me ask a question on that slide.

MR. BEARD: May I add one thing? Be sure to address it to my boss. His name is Harold Denton.

MR. RAY: Also to Mr. Palladino. That's his boss.

MR. EBERSOLE: I got myself all enthusiastic about this condition, demand, for instance, don't do a crash start unless you have high drywell pressure and so on, but then it occurs to me that the actual demand for real need on the diesel generator is so rare that unless you find an explicit reason that a fast start is less reliable than an ordinary start, that those starts don't occur often enough to make any difference. So what it really means is all you've got to do is during the testing have most of the tests start up with a lot of supervision, a lot of graduality, and again, while you almost never have a LOCA start, also you will have very few real starts.

MR. RYDER: Sure.

MR. EBERSOLE: So if it is a cumulative problem, this starting crash, you are not going to have a cumulative load to amount to anything even for those which don't require sudden service.

MR. RYDER: That's true. Currently we do it all the time no matter what, whether in testing or whatever.

MR. EBERSOLE: That's the point, we do it all the time.

MR. RYDER: We could do it on demand. However, if you still wanted to keep the fast starts on demand, fine. Let's move to testing, every fifth time, fine. We are taking a big chunk out of the wear, or even every other time. That still brings some reduction.

So anyway, there are a lot of different areas where I think we could just modify starting requirements instead of in addition to equipment.

(Slide.)

MR. RYDER: The last slide just says "The End."

MR. RAY: I think we anticipated that one.

Thank you, Chris.

I would like to make sure that I have the Subcommittee's support on my intent to suggest that if not a letter from Paul Shewmon to Mr. Palladino, at least a letter from Ray Fraley to the Executive Director of Operations would be in order conveying the suggestion for the Staff's consideration.

Do I have the support of the Subcommittee for this?

(Unanimous nods in agreement.)

MR. RAY: I would like to know if there is anyone here representing Warren Minners.

(No response.)

MR. RAY: Okay, thank you.

Srini, I think the podium is now yours, and I would exhort you to limit it to about 35 or 40 minutes.

MR. SRINIVASAN: I was here back in March giving a status report on the recommendations of NUREG-0664. That is the DC system reliability study. Since then, we have updated the branch position. The basis for updating this question was the receipt of comments from the NRR Staff, comments from the AF.

Before I turn this forum to my Staff, Mr. John Knotts, to go over the additional guidance we have put in the position, I would like to characterize the nature of the changes we have made in the proposed branch position.

As we all know, the study -- system reliability system -- concerned a minimum two divisional system. In practice, if you look at the majority of the plants we have been licensing recently, it far exceeds the minimum in the particular study. Things like Class 1E division, full Class 1E divisions, we see dedicated battery for the BOP functions. We see separate switch yard batteries.

So the Staff has determined that there is some benefit to including these current practices as well in these guidelines, along with the surveillance requirements, the seismic criteria, the interfaces with 1E and non-1E systems. So the question you have in hand that is dated 7/30/82 contains a more comprehensive DC system position.

What we intend to do with this is to find out how much of this we will require on the earlier designs which do not have all of these features which we have on this particular position. That requires an exercise on cost-benefit analysis.

We are starting on a program with EG&G on the cost aspect of these various requirements and Pat Baranowski, the task master of the DC systems study, will be doing the benefit aspect. I think he is currently doing some updating of his data to achieve greater certainties in the data he has got.

Hopfully, these two actions will be completed by the end of November. We are anticipating to go before CRGR in the month of February. After their review and comments, the process requires us to go to the public for comment, and back again after resolution of the public comments to CRGR to finalize the requirements.

MR. RAY: That is, you will be submitting the BTP after it has been through the Staff mill for public comment?

MR. SRINIVASAN: That is after the CRGR process. There are two processes that are involved -- one after we do the cost analysis. We have to go justify how we are going to implement these requirements in the various classes of plants. As you have seen in one of the slides, we tried to look at it from the earlier reactors, current NTOLs, and any future new designs. We have to go through the cost-benefit analysis before you put any new requirements on beyond the current regulatory requirements.

After that process is done, we intend to go out for public comments. That will be sometime in March or April. So my next appearance here will be around -- it happens every six months, so I would think I would be here around March or so, at least giving you a comprehensive position with the cost-benefit analysis prior to the public comments.

MR. RAY: Repeat again for me. You would be in a position, you anticipate, after Staff performances, to submit the BTP to the public for comments in March?

MR. SRINIVASAN: March.

MR. RAY: And after having processed those comments you anticipate what kind of a schedule or service date, if I might use the term, for the BTP in final form for Commission approval?

MR. SRINIVASAN: I would require -- It would require CRGR approval as a requirement to various operating reactors.

MR. RAY: With the CRGR approval, you can then lay it on the industry?

MR. SRINIVASAN: Yes.

MR. RAY: When do you think you might have that again?

MR. SRINIVASAN: That would be at least a year away, by the time we wrap up all the resolution of the industry comments and put the final package through the CRGR.

MR. RAY: You know, sometimes I understand the frustrations in the industry as to why in thunder it takes so long for things to move. Inertia is there.

MR. SRINIVASAN: Mr. Ray, there are a number of things which the Staff is doing. Each one is prioritized and we give enough resources for this one, closely followed by Pat's work on station blackout, and in-between we are trying to get to the DST program on the assessment of reliability of reactors.

MR. RAY: What you are saying is you are staff-limited.

MR. SRINIVASAN: Yes.

MR. RAY: So is the industry, very severely.

I would like just a couple more minutes from you on what considerations dictate a branch technical position as the medium for imposing these requirements on the industry. Why not a GDC or some other mode of requirement?

MR. SRINIVASAN: The BTP need not go to the Commission level. It can be done, usually, within the office itself, within NRR. This is prior to the CRGR establishment. Since there are new requirements in this BTP and we need to do a cost-benefit analysis, we have to go before the CRGR. This is the shortest and most quickest way of getting things out.

It is regulation. Like if you wanted to put a new GDC, it has to be a rulemaking and you have to go before the Commission.

MR. RAY: Horrors! You have said enough.

MR. SRINIVASAN: And also, I believe, the guidance of the requirements we are putting in are not that significant enough to go and change the regulation. They are merely reflecting what the industry is practicing on current designs.

I would like to see some of them being sort of backfitted on the earlier designs.

MR. RAY: Okay. Any questions?

(No response.)

MR. SRINIVASAN: If I do not have any more questions, let me ask my Staff, Mr. John Knotts, to go over the current status of the position.

(Slide.)

MR. KNOTTS: Okay. To start off, I am going to have a rewrite of what we had on our March 30 meeting, so I will just go over it very rapidly from where we were at the end of the March 30 meeting.

First of all, recommendation 1, prohibit design of operational features which could compromise division independent. Basically, we have proposed interconnections between redundant divisions accomplished by manual means only, restricted to cold shutdown and refueling, be kept under strict administrative control, meet single failure designs such that there is two series disconnect devices that are alarmed if they close, and also we are proposing some kind of restriction between DC systems at multi-unit plants.

(Slide.)

Position 2 deals with multi-action plant items, which basically will get better enunciators, better monitoring of the DC systems so the control room operator has immediate knowledge if the battery fails or is available. So we propose alarms and monitors for the control room, and also we are proposing that failure of one battery bus not cause total loss of the control room enunciator system.

MR. EBERSOLE: May I ask under the second bullets -- items 2 and 3 -- that is an instantaneous reading. Why don't you integrate that and have a cumulative exhibit of the residual charge -- input, output? I am saying if you integrate that and get the difference, you will have something that tells you, apart from hydrometer readings and so forth, where the battery stands.

MR. KNOTTS: Yes, we could do that. That could be done.

MR. EBERSOLE: Well, it is just a thought to kind of scratch on the slide.

MR. RAY: Might not this be more significant to the operators?

MR. KNOTTS: As far as the availability of the battery on demand. It would not help him after the accident happens.

MR. RAY: No, but it would tell him how near the brink he is.

MR. EBERSOLE: It would have stopped a number of our experiences, where the battery was found it had been drained unknowingly.

MR. KNOTTS: We have an alarm when you start getting a battery discharge.

MR. EBERSOLE: That is truly closing the door after the horse is out.

MR. MAC AVOY: That device you are mentioning is standard on nuclear submarines.

MR. EBERSOLE: Oh great. We have a fine precedent.

MR. RAY: Therefore, it is brought in by Rickover.

MR. MAC AVOY: It is useful. I found it helpful.

MR. SRINIVASAN: Mr. Ebersole, what we see with regard to monitors is the current practice. These are what I would take as a guideline, the refinement or sophistication of more useful information. What we have seen is always welcome. We are not rigid that we should have one for the input, one for the output. If you want to integrate it, that is fine too.

MR. RAY: You would not object, is what you are saying, if a licensee came back and said I want to indicate the state of the battery rather than these things, or would you want in addition to these things?

MR. SRINIVASAN: One could compare what is being proposed against what we have as a requirement, and that is always done in the licensing process.

MR. RAY: It is open to negotiation?

MR. SRINIVASAN: Yes. If you see the question as some licensing guidance, we would like to see some critical parameters to be monitored, and I see a lot of interesting gadgets coming out to even monitor the availability when it is connected to the bus. But we do not want to go and specifically say we would like to put those instruments in some of the earlier reactors, where you do not have any space in the control room.

We would like to leave the option to the initial designer and the licensee to come up with some monitoring system which will tell you the status of the battery and its current situation -- whether it is discharging or it is holding its charge.

MR. RAY: Post-TMI, certain requirements were specified to -- in the way of instrumentation and enunciator and so on for an operator to control the progress of an accident. Were any of these involved in those additions? These are over and above those?

MR. SRINIVASAN: Yes. It is so interesting. The TMI only two items that came to the power system branch. One, as you recall, is the power supply to the pressurizer heaters. The other is the power supply to the indication of the PORV on the pressurizer level. Those are the two impacts we had on these two particular disciplines.

This is coming from the generic study. At

TMI, I think, the battery was all right.

MR. RAY: I could not possibly remember that list, but I just wanted to make sure that you were not duplicating something.

MR. SRINIVASAN: No. There is one item you will see later on which is the bypass inoperable status of a DC system. If you operate opening the breaker on the battery charge going to the bus, that has to enunciate in the control room. Reg Guide 1.47, TMI action plan, establishes that, and we have that requirement in here. But that requirements has been in for a while.

TMI sort of reinforced that we should have a bypass inoperable status indication in the control room.

MR. RAY: What you are saying in that instance you are providing another reason for having it.

MR. SRINIVASAN: Right.

MR. EBERSOLE: Is there enunciator window that goes on when the battery output current begins to depart from zero or any other kind of signal that says you are emptying the bucket?

MR. KNOTTS: Well, you have got DC bus under-voltage.

MR. EBERSOLE: I know, but that requires too much intelligence. I want to know when I start draining my charge. Shouldn't I have flashing lights that says you are now on a collision course unless you stop sometime?

MR. KNOTTS: You have a battery discharger alarm that should give it to you.

MR. EBERSOLE: Is that another one where it tells you are all finished?

MR. KNOTTS: No, when you start discharging.

MR. EBERSOLE: Oh. Well, that is what I really meant. Right. So you say when that goes to something more than zero, you get a light or something?

MR. KNOTTS: Right.

MR. EBERSOLE: Oh, yes, battery discharge.

MR. KNOTTS: Normally your input for it would be --

MR. EBERSOLE: Okay.

(Slide.)

MR. KNOTTS: Okay. Position 3 is inoperable indication for the battery output breaker and the charger input and output breaker. If you open those for maintenance or for any other reason, for tests, for operability checks on the battery, it should be indicated as part of your bypass inoperable status indication system.

MR. RAY: What do you mean by DC system bypass? I am missing something.

MR. KNOTTS: You take the battery, the DC system, out of service for maintenance or tests. We open the breaker to do the testing.

MR. RAY: You lock it out.

MR. MAC AVOY: Is there a battery output breaker on stations now?

MR. KNOTTS: Some do, some do not.

(Slide.)

Okay. Recommendation 2 -- the NUREG. You want to minimize the likelihood of battery damage due to human-related common cause failure.

Position 4 has written procedures and administrative controls to prevent the activities on redundant divisions at the same time, requiring review of activities to minimize human error, causing more than one division to be unavailable, and assurance that activities are done correctly -- for example, the rotation of personnel or verification of completed work by other qualified personnel.

MR. EBERSOLE: Let me ask on that second line, minimize the potential for human error. Carry on, I am sorry.

(Slide.)

MR. KNOTTS: Okay. The preventive maintenance on bus connections and DC power availability from the battery to the bus. We have included in our standard technical specifications, and we are also going to include or we do include visual inspections and measured resistance of battery and bus terminal connections and battery service tests.

(Slide.)

MR. LIPINSKI: Mr. Chairman, will we hear on the paper about measurement of bus connections? That is on our agenda as one of the last items.

MR. RAY: You mean the high resistance conditions and so on? John McAvoy is going to have the opportunity to make a few statements.

MR. LIPINSKI: Okay, then I will not bring the issue up at this point.

MR. RAY: You might then.

(Slide.)

MR. KNOTTS: Recommendation 4. Through administrative procedures and operational, we want to maintain reactor core cooling given the loss of any DC bus and a single independent failure. We have position 6A, which basically we are going to do an analysis of the DC system to assure that given the DC system failure with the independent failure and shutdown cooling system we still have the capability of shutting down the reactor.

Considerations and assumptions for this analysis will be the duration of the DC system, venting out, transient conditions and interaction, system and components associated with failed bus being unavailable for shutdown cooling, and they should not be considered as independent failures. Failure of the redundant DC system need not be considered, assuming that you meet the first five positions.

Shutdown systems and components will be safety grade, used regularly or subject to routine operability checks and a single failure means a single active failure. We are not talking of passive failures in this case.

MR. EBERSOLE: Before you leave that, of course, it would be a lot more conservative if the failure of one DC bus did not put a demand on the shutdown cooling functions in the first place. But here you have carried it to the point where that has been permitted to occur.

Now since you usually have the minimum configuration of two trains at the 4160 level, does this imply that the failure of -- and usually, by the way, the 4160 DC control systems come off the individual batteries -- does this imply you are going to have a swing battery or something to pick up the function of the corresponding 4160 services, so that you can then allow failure of the 4160 level?

MR. KNOTTS: We are assuming that you take the failure of one DC system, which would mean -- one DC system would mean the failure of one 4160-volt system.

MR. EBERSOLE: Right.

MR. KNOTTS: We are not going to take the failure of the redundant battery associated with the other 4160.

MR. EBERSOLE: What am I now going to do? Having failed that 4160 system when I fail a 4160 pump on the other bus?

MR. KNOX: In that case, you wouldn't have the redundant capability of shutting down the plant, and you wouldn't be able to meet the analysis.

MR. EBERSOLE: So you shouldn't have it shut down in the first place, or else you are going to have an alternate DC supply for that 4160, and other such services that require DC support, which means three batteries.

MR. KNOX: Or other systems that don't require DC batteries.

MR. EBERSOLE: Or other systems that require DC controls or something like that.

MR. KNOX: Right.

MR. EBERSOLE: Well, okay. All right. I just wanted to understand what you meant here.

(Slide.)

MR. KNOX: Okay. Now we get into our alternative to the analysis that we propose in Position 6A. We have a Position 6B, where we are going to propose another balance of plant DC battery system to provide power to the normal shutdown cooling loads that would be independent and separate from the Class 1E battery and its loads. We are also proposing an independent DC system to supply the shipyard and off-site power control circuits.

So, basically, we have one balance of plant battery, two switchyard batteries, one for each of the off-site power circuits, and then the two Class 1E batteries.

MR. EBERSOLE: Is it pretty much implicit in your requirements now that you are going to agree to two DC buses as a minimum which disallows the thesis of two bus failures, but you may be requiring a standby DC supply consisting of rectifier and battery to swing in and take the loss of a DC source on a previously working bus?

MR. KNOX: No, we are proposing a separate and independent DC system to handle the control power needed for the normal shutdown cooling.

MR. EBERSOLE: Even the bus?

MR. KNOX: The total system, that is right, will be independent.

MR. RAY: I don't remember that being part of the original recommendations of NUREG-0666.

MR. KNOX: That's correct. This is an alternative proposal from a DC systems point of view. We are trying to come up with an alternative suggestion versus a system analysis.

MR. RAY: Yes, but let's think with the original and not consider an alternative. Suppose this alternative isn't elected. Then what is required in your BPT?

MR. KNOX: If Position 6B is not --

MR. RAY: Would 6A then satisfy it?

MR. KNOX: Six A would satisfy the recommendations. That's correct.

MR. RAY: Okay. It just wasn't clear to me.

MR. BARANOWSKY: It may be easier for someone to go to 6B than to go to 6A. A licensee, for instance. Personally, I would go with 6B, but the risk and reliability analyses indicate that 6A provides a consistent level of safety at the plant. It is not an optimum way to go about doing things, and if I had the choice of being a designer, I would go with the additional batteries that they are talking about in Position 6B.

MR. EBERSOLE: Pat, when you say batteries, you really mean integral DC systems, don't you?

MR. BARANOWSKY: Yes, I do.

MR. KNOX: For this non-Class 1E battery we are proposing, we have added monitoring and also recommendations for sizing. Position 7 is sizing of the safety related DC systems. Basically, the recommendations for the sizing, there is nothing really new about it, Position 7.

MR. EBERSOLE: In the non-safety DC systems, it is implicit that your intent here is to get all these parasitic loads off the DC batteries, but it is not explicit. Is that what you are going to require?

MR. KNOX: I have got a specific position as part of that that requires that all non-safety loads except critical loads be separated from the Class 1E batteries, and critical loads would be the lighting where communications systems that would be critical for shutting down the plant.

MR. EBERSOLE: Yes. Well, it is a little looser than I -- it is not in the nature of a hard line statement that you will shed parasitic loads off the 1E batteries.

MR. KNOX: We have a position that says only critical loads connected to --

MR. EBERSOLE: Okay.

MR. SRINIVASAN: Mr. Ebersole, it is on Page 11 and 12, as to what one should do if you should have some critical loads, non-safety critical loads on 1E buses.

MR. KNOX: Position 8 was the number of safety related DC systems. This is where we are proposing on new plant designs to have one battery per instrumentation channel, so that given a failure of one

DC system, we should not get a reactor trip which would cause the demand for the systems to operate.

MR. RAY: Your words, the meaning of them, Position 7, sizing of DC safety system, what you are saying, I read there, is that in the document that will go out, you will indicate the basis on which this DC system is sized. Is this so?

MR. KNOX: I believe so, yes.

MR. RAY: You will write a specification under Item 7, for instance, to determine the size of the battery capacity needed?

MR. KNOX: The sizing is basically a recommendation as we wrote it out in the position.

MR. RAY: Okay. So what I am saying is that in the final document you will have words in here that convey the sizing requirements, the basis on which it is sized.

MR. KNOX: Right.

MR. RAY: This isn't the finished product.

MR. KNOX: The position is written up in detail.

MR. RAY: In the document dated July 30th?

MR. SRINIVASAN: On Page 12, there are some criteria laid out for the Class 1E system sizing. It not only talks about design basis events, but also brings in the subject of the discussion this morning, station blackout. I think the batteries should be sized for both events.

MR. BARANOWSKY: In the original NUREG-0666 study, we deferred the issue of battery sizing due to station blackout because it will be addressed now.

MR. EBERSOLE: In that matter of sizing, let me ask you to at least see whether it is ar, good or not to give some consideration to engineered DC chargers. It strikes me that that might be a practical resource to monstrous batteries, considering how infrequently you will need it.

MR. BARANOWSKY: I think what we will be doing is laying out the reason for having battery capacity, so that someone could meet the intent of sizing, and that should be fine.

MR. KNOX: We have prepared a matrix for the options.

(Slide.)

MR. KNOX: Operating reactors, new term OL and CP plants, we are proposing to apply Position 1 through 5 or Position 1 through 5 and Position 6A, operating plants, and for OL plants that we are currently reviewing, we have the Option 2, 3, and 4, which will basically be either Position 1 through 6A, which would include the analysis, or Option 6B, or Positions 1 through 8.

For new plants, we would propose that the plants meet all the positions.

MR. EBERSOLE: Give me an idea of what the relative cost of a set of batteries is compared to the set of diesels. Would it be like 10 percent of the cost of the diesel set?

MR. KNOX: I am not familiar with the cost of the diesels.

MR. RAY: Didn't I see a figure this morning some time that a diesel might cost $30 million or $40 million?

MR. BARANOWSKY: Let me tell you about the cost of the diesels. First of all, you have to talk about where you are going to put it. The same might be said for the batteries. You have to talk about how difficult is it to wire the diesel or the batteries into the plant and does the plant have to be shut down in order to do that. At $500,000 a day for the cost of replacement power, that is where a lot of the cost of these systems comes in. In addition to that, you are talking about seismic buildings and safety grade quality work that costs a few bucks when you start adding hardware like that, whether it is battery or not.

MR. RAY: But, Pat, you can make these changes during the refueling. You don't have to penalize yourself about a half million dollars a day.

MR. BARANOWSKY: That would be true if we didn't have a huge number of changes going on right now during the refueling for about the next few years as a result of Three Mile Island. Utilities have said, if we will either let them go on some requirements or replace them with others that are more valuable, they would buy that, or if they will let us go three or four years into the future on backfits, they would buy that much more gladly than extending an outage say two or three weeks.

MR. EBERSOLE: Pat, my whole thrust in asking was this. I would call it the philosophy that we ought to have solid gold cotter keys, if that is the best kind of metal to make cotter keys out of. They don't cost much, and yet they keep the plants stitched together. So, just as a non-consideration of the economics is improper. If you buy a piece of safety for a nickel, you buy it. I don't care if it is against the moon hitting the station.

MR. BARANOWSKY: That is a good point, and I have to tell you that the cost information is going to be generated by EG&G Idaho. All that my people are going to be doing is developing the reliability and risk reduction changes associated with any of these positions being applied to operating reactors or OL's.

MR. SRINIVASAN: Mr. Ray, we recently asked a licensee how much it would cost to add a Class 1E battery system. It is going to be a very small percentage of the number he spends for the diesel, but I don't want to give any figure out until we do a systematic cost analysis.

MR. EBERSOLE: I thought as much. That is why I raised the question.

MR. RAY: Thank you very much. Are there any questions on this part of the presentation that have not been voiced?

(No response.)

MR. RAY: Okay, John, if you are prepared to make your comments, I would appreciate them at this time. I would like to introduce John McAvoy, a Fellow on the ACRS staff who has some concerns and some thoughts on the resistance of connectors between cells, et cetera, and batteries.

MR. MAC EVOY: I would like to discuss why this requirement to do battery terminal resistance checks is giving us a false sense of security because it is not telling us what we think it is.

(Slide.)

MR. MAC EVOY: Every year, the power station is required to measure the intercell connector resistance. I draw a picture of a battery. The intercell connectors are copper straps. They've got a little lead coating on them to make good contact, and they connect to two terminal posts generally on most of the batteries I have seen. These terminal posts are connected to the plates down in the cell, and this would connect, say, the negative to the positive in the next cell, and here positive to negative. All the cells are connected together. You have about 60 of them. And then they are connected to the bus eventually.

The utility is required to measure the resistance between the intercell connector and the terminal. That is all they are told to do. If the resistance is within 20 percent of the average value for the battery, then it is okay. They go on to the next one. They don't have to do anything. If it is not, they take the connection apart, they slap a little special grease in there, they retorque the connectors and check it again.

Now, when they are doing this check, they don't have any guidance as to where to put their probes. I drew an equivalent resistance just to show you what the circuit looks like. You can take an ohmeter probe, put a connector on the strap. You can put the probes over here or over here or over there. There is no guidance (indicating). And they have been doing all of the above, getting different resistance value, depending on where they put their probes.

I have worked out some values based on typical resistances here. This runs about 50 micro ohms. Another aside problem, there is no guidance as to how precise a meter they have to use. They can use a volt ohmeter accurate one ohm if they want to, and they will never get a reading that is 20 percent above the average, because it will always be zero unless the thing is open circuited, so we should give them a little guidance there, but the problem comes in when they go to measure the resistance. Say they stick the probes across here. Well, if you look at this, let's say we open circuit here, we open circuit there, we open circuit here (indicating), and we leave one moderately good contact, say, 100 micro ohms down here. So all of our current is flowing out of the batteries through this connector.

By the way, these terminal posts are connected inside the battery. I show them shorted right there. If a fellow comes up with his probes and he measures the resistance right here, which is perfectly acceptable, he is going to measure a good resistance even though it is open circuited and this contact is doing nothing. He will measure good resistance, because what is he measuring? He is measuring the resistance through the other intercell connector back through his good contact.

So, we have three out of four of the contact surfaces open circuited, and he gets a good reading. I worked up some of those numbers. There is no sense really putting them up on the screen, but let's get the one where they are worked up with three out of four contacts open circuited, infinite resistance, and the fourth one a bad resistance of 100 micro ohm, which is tolerable, not too great, but it is not too bad, either. He will come up with readings of 150, 100, and 50, 150, 100, and 50, if he puts his probes in those positions.

So, that cell is going to check out perfectly acceptable, and all he has got one square inch carrying up to 1,000 M's through that battery. It is also possible to have the entire circuit open circuited. This is fairly improbable, but you can do it and still come up with good readings. Open circuit right here due to a faulty connection, and open circuit right here (indicating). If he takes his resistance values in the right way again he will come out with the fact that he has got good terminal resistance. He just measures right here, aha, that one is good. He measures this one right here, aha, that one is good, but what has he got? He has got an open circuited battery.

So, because of considerations like that, I would say we should probably discontinue the current method of how we take our battery cell resistance readings. There is also a complicating factor I didn't bother to throw up here. There is a bolt through this terminal and a bolt through that terminal, and a bolt through this one, and a bolt through this one, which in effect is just another resistor from this connection or from this strap to this strap (indicating). That provides another trunk of resistance to make the connector look good, but it has nothing to do with connecting the connector to the terminal.

So, again, it will check out even better when you've got open circuits in here. I could sort of open it to discussion as to how we really should take these readings.

MR. BEARD: John, could I ask a question? I am struck by one thing you are saying, if I read you right. That is, basically, that there is a requirement that has a good basis for it that says we ought to be determining what the terminal resistances are from time to time so that we have a problem and don't know about it.

MR. MAC EVOY: Right.

MR. BEARD: I think the second thing you are saying is, depending on training and intent, and how the guy's wife treated him the night before, and everything else, he can get any reading he wants.

MR. MAC EVOY: Right.

MR. BEARD: Then I think your conclusion is that we should withdraw the requirement.

MR. MAC EVOY: Wrong. It is not that the guy is saying he is going to go out there and see an open circuit and say, I will make it look good. He can go along and say, I will read this one, I will read that one. He is not measuring this battery. He is measuring that one over there. He only thinks he is measuring this one. It is the ambiguity of it that bothers me.

MR. BEARD: I think your attempt is to specify how to do this.

MR. MAC EVOY: There is no way to do it that I come up with with an ohmeter.

MR. EPLER: Question. Why doesn't somebody tell the designer that redundancy in parallel circuits are no good unless you can test them independently? That is in the primer.

MR. MAC EVOY: Right. I just don't think anybody has noticed this.

MR. EPLER: This is in the primer. Why did it take so long to find out?

MR. MAC EVOY: Right now our tech specs say, measure in accordance with IEEE. IEEE says, measure resistance but nobody knows they are measuring the wrong resistance here.

MR. BEARD: I guess, John, my whole basic point for bringing this up, and he brings up the same one, is the basic requirements are all there, and really I think what you are trying to say is, when you do this, don't screw it up, do it right.

MR. MAC EVOY: There is no way to do it right that I have come up with.

MR. LIPINSKI: You wrote the equation through the closed loop, but you didn't give the inverse solution. You had four unknowns and you had four measured quantities. By rearranging those equations, you can solve them for the four unknowns. Do you have your equations on the vu-graph?

MR. MAC EVOY: No, I will have to think about that. I will give you the memo.

MR. LIPINSKI: I have the memo. That is why I am making the comment.

MR. MAC EVOY: I am not sure you can go back like that.

MR. LIPINSKI: There are a non-linear algebraic set. If it were easy, I would give you it now, but by iteration you can solve that non-linear algebraic set and find the unknown resistance is that you are interested in.

MR. MAC EVOY: I don't think you can, because these two are in parallel and those are in parallel, and how are you going to say what contribution this has to that parallel set? I don't think you can do it.

MR. LIPINSKI: But by working the inverse set, you could have gotten the measure you are interested in, namely, the continuity between the bar and the post. You can make a series of measurements and then knowing what that circuit is based on the measurements you are getting, you can then solve for the inverse numbers.

MR. MAC EVOY: I will agree with you, if you know what these resistances are, but there is no way of measuring these other resistances.

MR. LIPINSKI: But you have got to go from post to bar, post to bar, post to bar. You get enough of your measurement points that are different, and then when you rearrange the equations, you can get the resistances of interest.

MR. MAC EVOY: It would be fun to sit down and talk about that, but the thing is, right now what is being done is, they are just measuring. It is not measuring anything that is useful.

MR. LIPINSKI: I was rather surprised, because you carried your paper to a point, but you didn't continue it and provide the solution, and you had the solution.

MR. MAC EVOY: The solution is almost useless right now, because what are they doing out there? They are measuring values that we have no idea what they will be used for.

MR. LIPINSKI: I will look at your paper and convert.

MR MAC EVOY: It is high school engineering. I am sure there is no problem with that. But we have got to revise the test as it is being done right now, is what I am trying to say.

MR. LIPINSKI: I agree with you.

MR. EBERSOLE: Isn't it a case where an attempt to be non-prescriptive the test is non-prescriptive, and the interpretation is simply no good at all?

MR. MAC EVOY: Right.

MR. EBERSOLE: So what do you do? You have to be prescriptive.

MR. MAC EVOY: Well, that is right, but I don't know that by being prescriptive, by using the methods right now.

MR. EBERSOLE: That might be another method.

MR. MAC EVOY: We have got to come up with a unique solution to this.

MR. EBERSOLE: What would happen if you took very accurately sensitive thermal tape and put it on these things and then ran a charging card through it which is uniform as a series circuit? Would you see a temperature difference at the points where you ought to?

MR. MAC EVOY: Let me take it one step further. What I would suggest as a solution is just to load the battery and do an infrared scan.

MR. EBERSOLE: Same thing.

MR. MAC EVOY: And pick out the connections that are hot.

MR. EBERSOLE: Put it on the charge load.

MR. MAC EVOY: Either one, but that is the only solution I can think of without going into all sorts of calculations.

MR. EBERSOLE: They really do have some very fine tapes now that discriminate to some degree.

MR. MAC EVOY: That would do it also. I didn't note their existence.

MR. EBERSOLE: They do it for patients in hospitals.

MR. BARANOWSKY: I think one of the interesting things to reiterate here is, you are talking about having a general requirement such as might exist in an industry standard that is so general and vague that when we come out at the NRC and say, make sure you check your resistances and a person says, hey, IEEE requires that, and we say, well, why are there failures then, and this is the reason. You have a very good idea, but it is not executed properly.

MR. RAY: There is a question in my mind as to the avenue of directions. Srini, should the IEEE standards, appropriate standards committee be induced to prescribe the way the tests are made, and the regulatory edicts as they now exist invoke that standard, preserved the way they are, or should the NRC take it upon itself to prescribe a method of test? Assuming in the meanwhile that by some analyses such as John and Walter are going to undertake, as I understand you are volunteering, a result that is of practical application possibility is reached.

MR. SRINIVASAN: In the normal regulatory process we lay requirements for periodic testing, but we do not tell the licensee how to conduct the test or to write the procedures for the test. In this instance, it is in the standard tech spec to verify the terminal connection of the resistance there.

MR. RAY: You say it is a standard tech spec?

MR. SRINIVASAN: Yes. It came out of the IEEE standard 450. It is there too. So people should know how to do it right.

So what I could do, not as a regulatory but as an individual person, is to go back to the working group, which is meeting sometime later this month, to find out if they know what is the correct way of measuring resistance.

MR. RAY: Then let us agree on this collectively that you will do that. You will run it down from your affiliation with the Standards Committee, and John and Walter will consummate the analyses that John has initiated in the memorandum he cited a moment ago, and we will touch base with each other -- that is, his committee and you -- at a future date to see what you have been able to accomplish and we can then maybe offer something.

MR. SRINIVASAN: John Knotts, who made the presentation, is a member of the working group and he will be attending the next meeting at the end of this month and I will definitely ask him to bring up this subject by the working group members and we could coordinate the efforts and see what the outcome is.

Let me add --

MR. RAY: Excuse me. One other point. John, it might be worthwhile for background for the other John to have a copy of the memorandum that you sent to us as an initial basis of background.

MR. MAC EVOY: Fine.

MR. SRINIVASAN: One other thing I would like to point out is this is not the only test which we require as a part of the surveillance test. If there is a discontinuity within the cells or between cells, it will show up in the other measurements or other tests which are required by the standard tech spec.

MR. RAY: What are they?

MR. SRINIVASAN: They are all listed there on the list we have. We also looked at some of the LERs recently. We found out where there was one instance where there was a bad connection between cells. There is only one instance I am aware of.

MR. RAY: Where are they listed, Siri -- in your document dated July 30? I will not let you off the hook.

MR. MAC EVOY: I came up with two LERs of overheated batteries. One caused a fire due to high inner cell resistance. I do not know what the failure would have been, but it did not cause fires.

MR. RAY: I think the minimum conclusion could be that there is trouble sitting out there waiting to assert itself.

MR. ANDERSON: Mr. Ray, may I make a comment? I am John Anderson from Oak Ridge.

I would like to relate a little experience from our research reactor experience with batteries. That is, we found basically all of the methods for measuring contact resistance unreliable and concluded that even if you measured a poor contact resistance it was not necessarily indicative of a poor connection. It might be an anomaly in the technique. And if we did not, it also was not an accurate and necessary precursor of subsequent high connection resistance.

We abandoned all attempts to try to measure this contact resistance and resorted to preventive maintenance, which has been totally successful. We simply take them apart and --

MR. RAY: And remake them?

MR. ANDERSON: Yes. And we have had no

failures that I am aware of in the past eight or ten years since we adopted that philosophy and abandoned the contact resistance measurement.

MR. EPLER: For how many batteries, John?

MR. ANDERSON: About five research reactors, in my experience.

MR. EPLER: How many batteries for one reactor -- nine?

MR. ANDERSON: Nine sets, yes. We have DC emergency cooling pumps as well as the instrument batteries, so there is about six or nine per plant, yes.

MR. RAY: So that is 30 to 45 batteries. In that evolution, Mr. Anderson, did you consider and try the infrared tests that were tried a moment ago?

MR. ANDERSON: No. We did not try the infrared. However, we went through a variety of resistance measurement techniques and temperature measurement techniques with contact measurements with no success.

The basic problem was that the measurement did not precede the failure in any connected fashion, that it would check good today and fail tomorrow.

MR. EBERSOLE: That is that place where time does not flow uniformly.

MR. RAY: Did you have failures?

MR. ANDERSON: Yes, indeed. We had chronic failures before we went to the preventive maintenance, cleaning and remaking the contacts. It was a serious problem.

MR. RAY: Thank you. I think this is a constructive contribution.

Well, we are not going to short-circuit or suggest short-circuiting the normal standards group. I think your suggestion a moment ago is an appropriate one, Srini, so if you go initiate that contact, in the meanwhile we will ask John to continue with his work and see what we can contribute.

MR. SRINIVASAN: Very good.

MR. EBERSOLE: John, how often do you take them apart?

MR. ANDERSON: I believe it is about every three months, but I am not certain of that.

MR. RAY: And that may be the course that the standards should dictate, Srini.

MR. MAC EVOY: I was trying to avoid that with the infrared check because he mentioned the other surveillance checks. I might get the time wrong, but you have an 18-month service test which does not load the battery a heck of a lot for a long time. It is just a very quick load which drops quickly.

MR. ANDERSON: Let me correct an impression. They do a battery set every three months, and they rotate through the six or nine -- whatever it it. Each one perhaps gets it once a year or once every year and a half.

MR. EBERSOLE: John, let me make a guess. Your batteries are in a research reactor, not these big commercial things.

MR. ANDERSON: They are not as large.

MR. EBERSOLE: I am getting into another point. When you test them, you probably do not need them. In these plants, we need all the batteries all the time to get redundancy.

MR. EPLER: Some are continuous.

MR. EBERSOLE: You do not have decay heat.

MR. ANDERSON: Yes, we do, as a matter of fact. We had the emergency coolant pumps are supplied from these batteries directly.

MR. EBERSOLE: Then you do degrade active systems when you test.

MR. ANDERSON: If we test on-line, yes. We do not have the continuous operation problem and we do make the test during shutdown. But they are capable of being done on-line through redundancy.

MR. EBERSOLE: Yes, through extra batteries maybe, but here, at least up to now, these batteries are in constant demand all the time. You do not want to fall back on single track.

MR. ANDERSON: Yes, I understand.

MR. MAC EVOY: It is done in an commercial plant where you are disconnected for the load test. You have to disconnect the battery and connect it to the load and meanwhile the plant is being picked up by the charger.

MR. EBERSOLE: Right, but that should be done --

MR. MAC EVOY: Yes, after long-term shutdown.

MR. RAY: Any comments or questions that have not been covered?

(No response.)

MR. RAY: Thank you very much, John. I wish you and Walter would pursue the thought you had, Walter, and see what might come out from an analytical viewpoint.

This, as far as I am concerned, completes the program for the day and although I did not anticipate it this morning, we are 40 minutes ahead of schedule and I would like to thank everybody that participated today, particularly the NRC Staff, the Oak Ridge boys, and --

they are gone, but the Sandia fellows. But you can convey that to them, Pat, and those in the audience, representives of the various users of the products that come out of these discussions.

I think a very frank and beneficial exchange of viewpoints has been taking place here today. I thank the Subcommittee members and for the general orientation of the Subcommittee members, it is my intent not to require a presentation on the part of the Staff to the full Committee of the proceedings today or a summary of them.

I understand that you must go through the CRGR before you really are in a position, if it were necessary or if it becomes desirable, to come to the full Committee with the story. Is that correct? Is that the requirement that is laid on you?

MR. SRINIVASAN: Yes.

MR. RAY: Okay. This, then, from that viewpoint, would not be an appropriate time for the Committee to get the story in a direct fashion. What I intend to do is to supplement the minutes which Dick Savio will write with a letter to the members of the Committee that highlights today's proceedings and conveys a copy of the branch technical position, in effect, to the members of the Committee so that they will know what is developing and thereby generate, if they feel it desirable, any comments that need to get back to you through us that might benefit you, rather than through normal channels.

By that I mean either a letter to the EDO or a letter to Mr. Palladino. Are there any misgivings on the part of any of the Subcommittee members on this point?

(No response.)

MR. RAY: Okay. Now do you have any significant comments that you would like to make? I add that first this morning I started this meeting with an intent to have such a letter drafted by tomorrow, but there is too much background here that I have not had a chance to read -- the complete reading of the document dated July 30, the BPT, for instance -- so it will be some time between now and the next full Committee meeting in October before that letter is finished.

A copy will go to you gentlemen and if you have any significant comments that you feel might help me in that chore, I would appreciate getting them in the meanwhile.

Thank you. Thank you once again. The meeting is adjourned.

(Whereupon, at 5:25 o'clock p.m., the meeting adjourned.)

NUCLEAR REGULATORY COMMISSION

This is to certify that the attached proceedings before the

in the matter of: ACRS/Subcommittee on AC/DC Power Systems Reliability

Date of Proceeding: September 8, 1982

Docket Number:

Place of Proceeding: Washington, D. C.

were held as herein appears, and that this is the original transcript thereof for the file of the Commission.

Jane N. Beach
Official Reporter (Typed)

Jane N. Beach
Official Reporter (Signature)

STATION BLACKOUT

UNRESOLVED SAFETY ISSUE A-44

P. W. BARANOWSKY
NRC TASK MANAGER

SEPTEMBER 8, 1982

T1

DEFINITION OF ISSUE

STATION BLACKOUT - THE COMPLETE LOSS OF AC POWER TO THE ESSENTIAL AND NON-ESSENTIAL SWITCHGEAR BUSES

USI A-44 - ARE THE LIKELIHOOD AND POTENTIAL ACCIDENT RISKS OF A STATION BLACKOUT HIGH ENOUGH THAT ADDITIONAL PREVENTIVE AND/OR MITIGATIVE MEASURES SHOULD BE REQUIRED?

PROGRAM APPROACH

EVALUATE AC POWER RELIABILITY

ESTIMATE STATION BLACKOUT ACCIDENT SEQUENCE PROBABILITIES AND CONSEQUENCES (RISKS)

COMPARE STATION BLACKOUT ACCIDENT RISKS WITH OTHER NUCLEAR PLANT ACCIDENT RISKS OR, IF AVAILABLE, WITH SAFETY GOAL AND DEVELOP OR REVISE LICENSING REQUIREMENTS AS APPROPRIATE

TECHNICAL PROGRAMS

TASK	PERFORMING ORGANIZATION
AC POWER RELIABILITY	ORNL WITH JBF ASSOCIATES AND EDG CONSULTANT
STATION BLACKOUT ACCIDENT SEQUENCE ANALYSES	SANDIA NATIONAL LABORATORIES
PLANT RESPONSE TO STATION BLACKOUT	EG&G, ORNL, LOS ALAMOS THROUGH RES/DAE SASA PROGRAM

MAJOR PROGRAM ELEMENTS

PROBABILITY OF STATION BLACKOUT

- RELIABILITY OF ONSITE AND OFFSITE AC POWER SUPPLIES
- STATION BLACKOUT CAUSE, FREQUENCY AND DURATION RELATIONSHIPS
- COST EFFECTIVE AC POWER RELIABILITY IMPROVEMENTS
- AC POWER RELIABILITY MONITORING

STATION BLACKOUT ACCIDENT SEQUENCE RISKS

- IDENTIFY STATION BLACKOUT ACCIDENT SEQUENCES
- RELIABILITY OF DECAY HEAT REMOVAL AND REACTOR COOLANT INVENTORY CONTROL SYSTEMS DURING STATION BLACKOUT
- DOMINANT FACTORS INFLUENCING STATION BLACKOUT ACCIDENT RISKS
- PLANT RESPONSE TO STATION BLACKOUT

STRATEGY FOR RESOLUTION OF ISSUE

DETERMINE "CURRENT" LIKELIHOOD AND LEVEL OF "RISK" DUE TO STATION BLACKOUT FOR A SPECTRUM OF PLANT DESIGNS

COMPARE RESULTS WITH OTHER NUCLEAR PLANT ACCIDENT RISKS AND SAFETY GOAL

IDENTIFY DOMINANT FACTORS AFFECTING "RISK" AND COST EFFECTIVE IMPROVEMENTS

- o AC POWER RELIABILITY
- o ABILITY TO COPE WITH EXTENDED LOSS OF AC POWER (CAPABILITY AND RELIABILITY)

PROPOSE NEW OR REVISED LICENSING REQUIREMENTS CONSISTENT WITH LEVEL OF RISK, SAFETY GOAL, AND COST EFFECTIVENESS

DEVELOP PLANT SPECIFIC IMPLEMENTATION PLAN

DEVELOPMENT OF LICENSING REQUIREMENTS

TECHNICAL IMPROVEMENTS INVOLVE DESIGN AND OPERATION

- o LCOs, TECH SPECS, SURVEILLANCE
- o PROCEDURES FOR TESTING/MAINTENANCE/EMERGENCY OPERATIONS
- o HARDWARE CAPABILITY, CONFIGURATION

GENERIC REQUIREMENTS WITH PLANT SPECIFIC IMPLEMENTATION PLAN

- o MINIMUM DESIGN REQUIREMENTS
- o DESIGN TRADE OFFS AND SPECIAL CASES
- o DETERMINISTIC

RECOGNIZE OTHER SYSTEM AND GENERIC ISSUE INTERFACES

- o EXTERNAL HAZARDS (SEISMIC, WIND)
- o FIRE PROTECTION REQUIREMENTS
- o SUPPORT AND AUXILIARY SYSTEMS CAPABILITY, RELIABILITY, DEPENDENCIES, AND INTERACTIONS

SCHEDULE

FINALIZE TECHNICAL REPORTS AC POWER RELIABILITY ACCIDENT SEQUENCE PROBABILITY	OCTOBER 1982
DRAFT NRC POSITION (PROPOSED RESOLUTION)	NOVEMBER 1982
INITIAL CRGR REVIEW	FEBRUARY 1983
PUBLIC COMMENT	JUNE 1983
FINAL CRGR REVIEW	SEPTEMBER 1983
FINAL NRC POSITION ISSUED	OCTOBER 1983

STATION BLACKOUT ACCIDENT ANALYSES

(PART OF TASK ACTION PLAN A-44)

ALAN M. KOLACZKOWSKI
ARTHUR C. PAYNE, JR.

SANDIA NATIONAL LABORATORIES
ALBUQUERQUE, NEW MEXICO

T3, T4, T5

STATION BLACKOUT ACCIDENT ANALYSES

OBJECTIVE: PROVIDE ACCIDENT SEQUENCE ANALYSES & RISK PERSPECTIVES TO RESOLVE USI-A44

EXPECTED DELIVERABLES:

IDENTIFY FACTORS LIMITING SHUTDOWN HEAT REMOVAL UNDER STATION BLACKOUT

IDENTIFY DOMINANT BLACKOUT ACCIDENT SEQUENCES, PROBABILITIES, & RISK PERSPECTIVES, & COMPARE WITH SAFETY GOAL

INVESTIGATE "OPTIONS" FOR REDUCING RISKS FROM STATION BLACKOUT

SCOPE OF ANALYSES

COMMERCIAL LWRs
    ALL PWRs EXCEPT EARLIEST DESIGNS
    ALL BWRs EXCEPT BWR-1 & LACROSSE

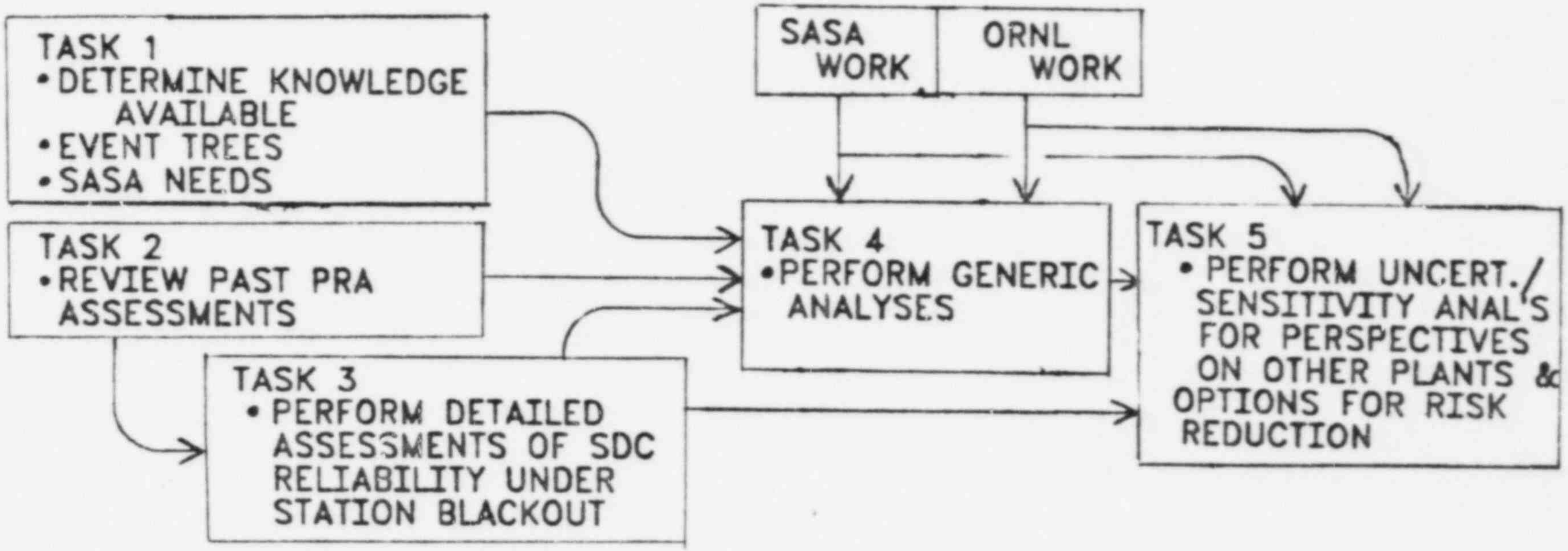
EXTERNAL EVENTS (SEISMIC,FIRE,WIND) TREATED TO THE EXTENT THAT INFORMATION IS AVAILABLE

USE OF AC SYSTEM CONFIGURATION & RELATED DATA FROM ORNL WORK

ACCOUNTED FOR LATEST DESIGN/OPERATIONAL FEATURES PARTICULARLY INCLUDING POST-TMI CHANGES

FAILURE TO SCRAM & INDEPENDENT LOCA SEQUENCES REVIEWED & FOUND RELATIVELY IMPROBABLE

MAJOR PROGRAM TASKS



TASK 1
- DETERMINE KNOWLEDGE AVAILABLE
- EVENT TREES
- SASA NEEDS

TASK 2
- REVIEW PAST PRA ASSESSMENTS

TASK 3
- PERFORM DETAILED ASSESSMENTS OF SDC RELIABILITY UNDER STATION BLACKOUT

SASA WORK

ORNL WORK

TASK 4
- PERFORM GENERIC ANALYSES

TASK 5
- PERFORM UNCERT./SENSITIVITY ANAL'S FOR PERSPECTIVES ON OTHER PLANTS & OPTIONS FOR RISK REDUCTION

ACTIVITIES RELATED TO TASK 1

CRITICAL REVIEW OF THE STATE OF KNOWLEDGE CONCERNING STATION BLACKOUT AT START OF PROGRAM

DEVELOPMENT OF EVENT TREES FOR THE PROGRAM & "UNIQUE" ASPECTS OF THE EVENT TREE MODELS

SASA PROGRAM INTERFACE & EXAMPLES OF SASA RESULTS

RESULTS OF CRITICAL LITERATURE REVIEW

PREVIOUS INFORMATION FOCUSED ON LOP FREQUENCY & DG RELIABILITY

PAST TREATMENT OF AC-INDEPENDENT SYSTEMS' CAPABILITIES & VULNERABILITIES FOUND TO BE INCONSISTENT IN PRAs

POTENTIAL IMPORTANT AREAS WORTHY OF STUDY INCLUDE:
- DC LOSS
- DIFFERENT PLANT SUSCEPTABILITIES
- BLACKOUT-INDUCED LOCAs
- HUMAN/PROCEDURAL ACTIONS

STATION BLACKOUT EFFECTS ON IMPORTANT PLANT FUNCTIONS

(LED TO 3 EVENT TREES)

	FUNCTIONS(SYSTEMS) REMAINING	FUNCTIONS(SYSTEMS) LOST
PWRs	DECAY HEAT REMOVAL (AFWS)	RCS MAKEUP (HPIS)
BWRs (2–3)	DECAY HEAT REMOVAL (ISOLATION COND.,APRS)	RCS MAKEUP (LPCS)
BWRs (3–6)	INTERIM HEAT REMOVAL & RCS MAKEUP (HPCI or HPCS/RCIC/ADS)	LONG TERM HEAT REMOVAL (SDCS,LPCRS)

Figure 1 GENERIC PWR EVENT TREE FOR STATION BLACKOUT

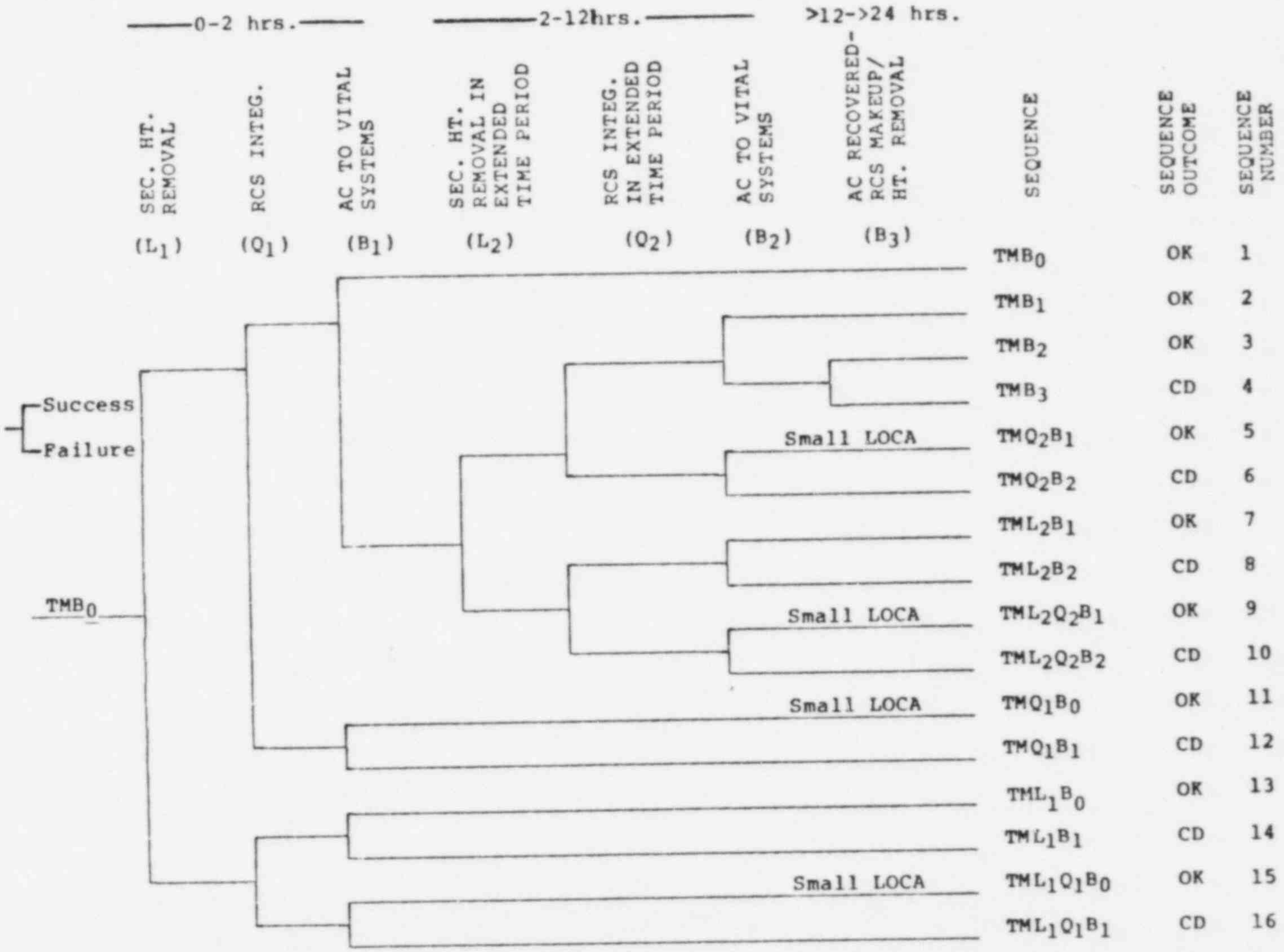


Figure 2. GENERIC BWR EVENT TREE FOR STATION BLACKOUT (BWR2 - BWR3)

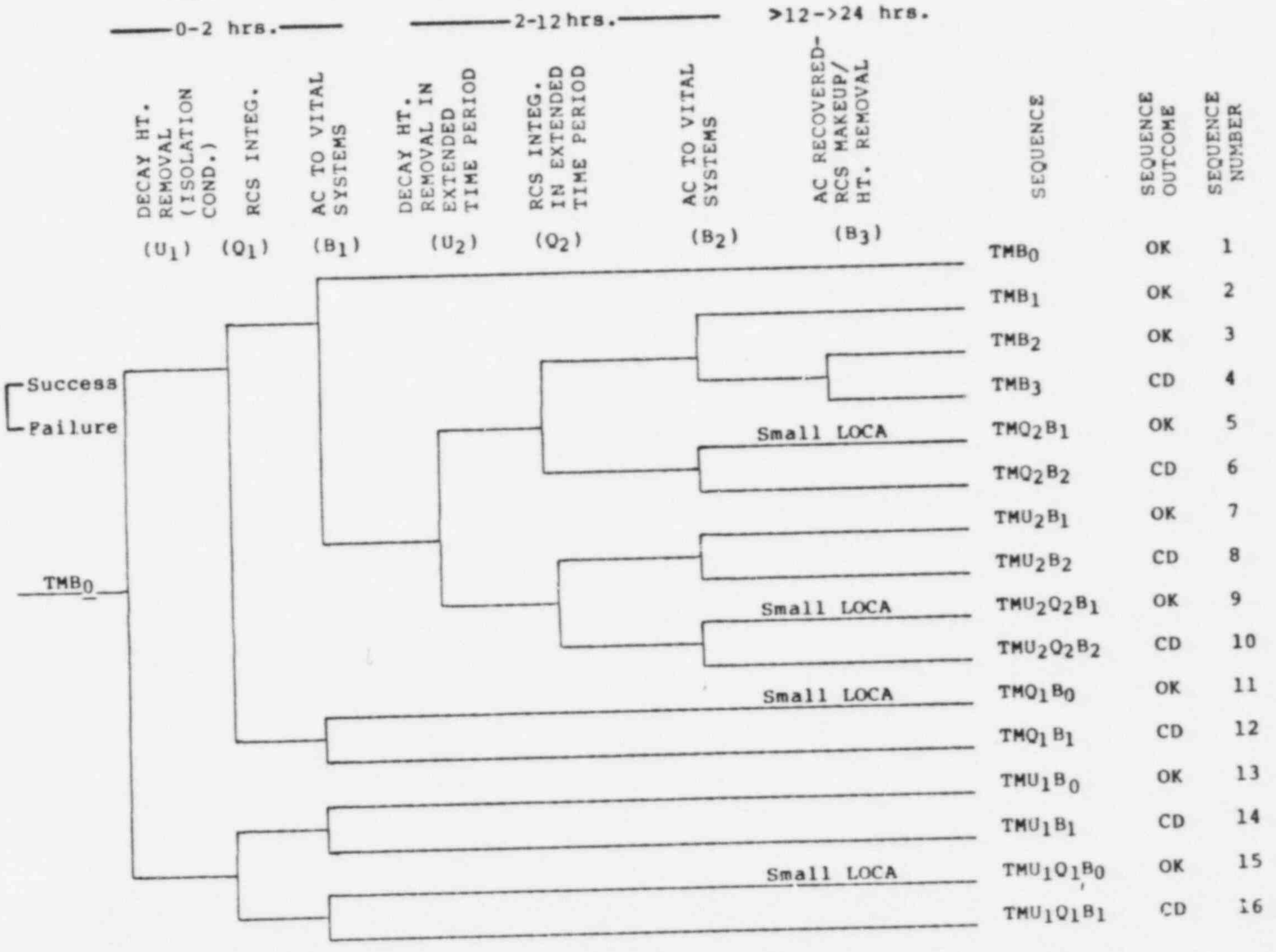
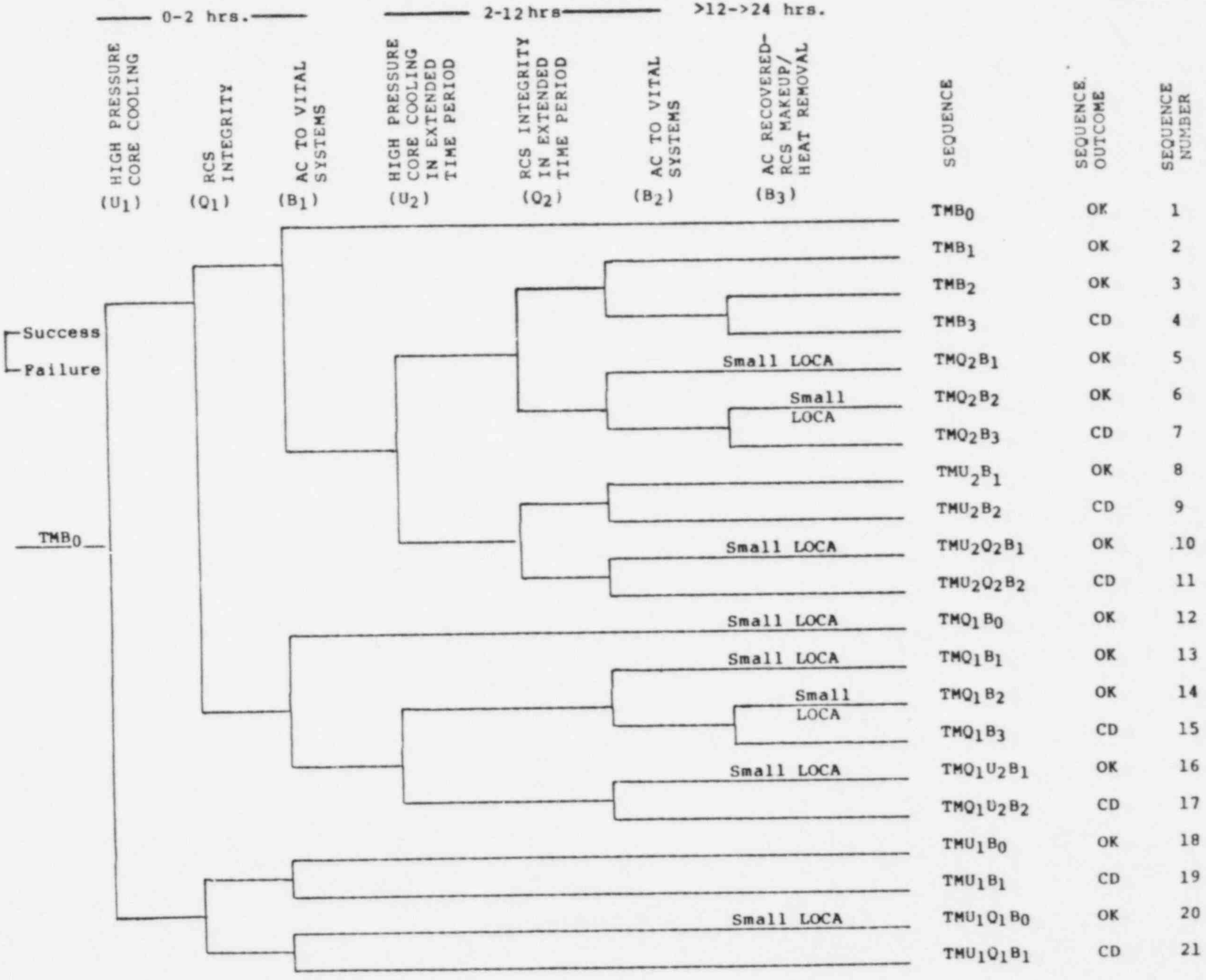


Figure 3. GENERIC BWR EVENT TREE FOR STATION BLACKOUT (BWR3 - BWR6)



SASA PROGRAM INTERFACE WITH STATION BLACKOUT STUDY

STATION BLACKOUT PROGRAM NEEDS:

- TIME TO CORE UNCOVERY/CORE MELT
- LAST TIMES AVAILABLE FOR ACTION TO PREVENT CORE UNCOVERY
- TIME HISTORY OF PROCESS VARIABLES
- SEQUENCE OF EVENTS

DETERMINE ABOVE FOR FOLLOWING CLASSES OF ACCIDENTS:

- ALL HEAT REMOVAL & MAKEUP FAILED, RCS INTACT
- AC-INDEP. HEAT REMOVAL OPERATING, RCS FAILED
- ALL HEAT REMOVAL & MAKEUP FAILED, RCS FAILED

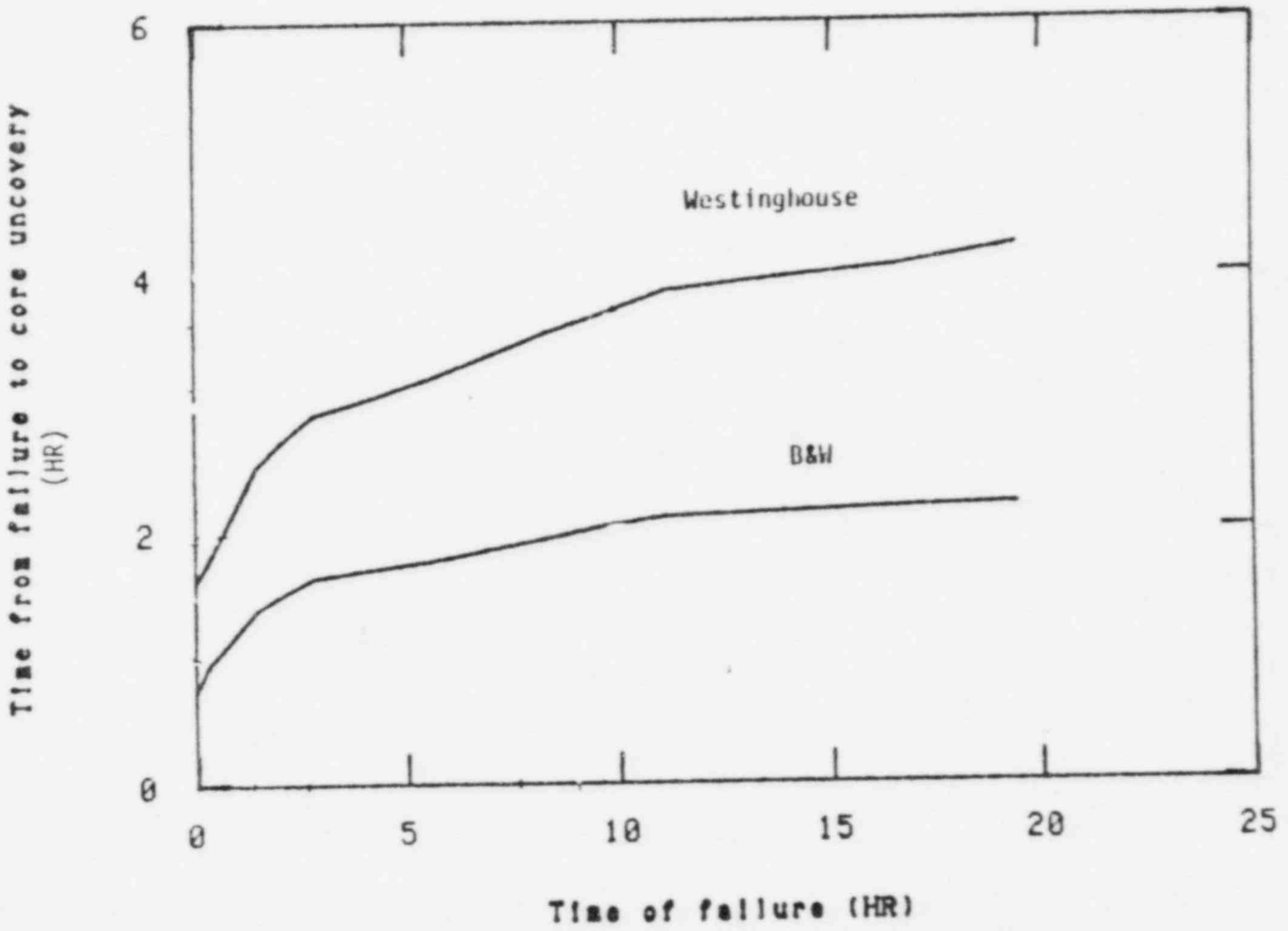
VARIABLES TO BE INCLUDED:

- PLANT DESIGN
- INITIAL RCS LEAK RATE & TIME OF RCS FAILURE
- TIME OF AC-INDEP. HEAT REMOVAL FAILURE

Table 6-1

Timing of MARCH Predicted Events for Zion TMLB' Base Case

Event	Time (minutes)
Steam Generator Dryout	81.8
Core Uncovery Begins	127.
Core Melting Begins	146.
Core Slump	180.
End of BOIL (Vessel Dry)	181.
Bottom Head Fails	187.
Containment-Pressure Spike	187.
Containment Pressure Exceed Lowest Failure Estimate	587.



Loss of offsite power, failure of all diesel generators, technical specification leakage, turbine driven auxiliary feedwater initially operates then fails at a later time.

Figure 6. Time to core uncovery as a function of time at which turbine auxiliary feedwater fails.

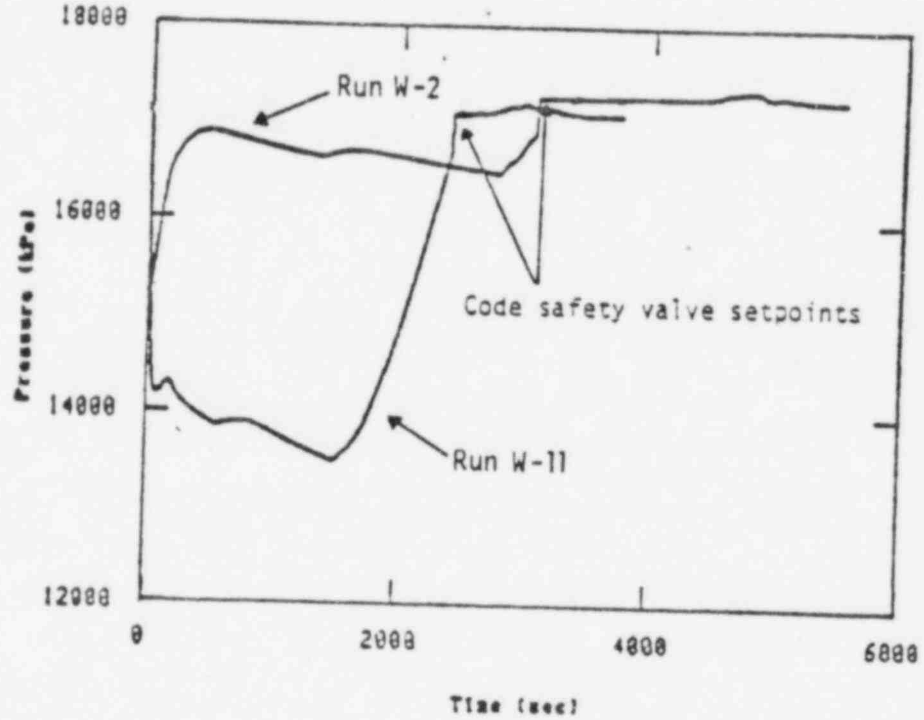


Figure 2. Runs W-11 and W-2 primary pressure vs. time.

Time (sec)	Event
3.5	Power generation due to delayed neutrons and fission product decay drops to 10% of initial rated power generation.
4.0	Feedwater turbines trip off.
5.0	MSIVs are fully closed, resulting in a momentary 0.69 MPa (100 psi) pressure increase and 1.02 m (40-in.) drop of water-steam mixture level due to collapsing of voids.
5.0	All control rods are fully inserted.
5.0	Reactor vessel pressure exceeds the lowest setpoint at 7.52 MPa (1090 psi) of safety/relief valves (S/RVs).
5.0	Seven (7) out of thirteen (13) S/RVs start to open in response to pressure rise above the setpoint.
5.2	Water-steam mixture level recovers 0.51 m (20 in.) from the previous momentary 1.02 m (40-in.) drop.
5.5	S/RV steam blowdowns into the pressure suppression pool through the T-quenchers begin.
7.5	Feedwater flow drops below 20%.
9.0	Feedwater flow decreases to zero.
10.0	Power generation due to fission product decay drops to approximately 7.2% of rated power generation.
15.0	All 7 S/RVs are completely closed.
15.7	Four out of 13 S/RVs start to open.
17.0	Neutron flux drops below 1% of initial full power level.
21.0	Narrow range (NR) sensed water level reaches low alarm (Level 4), i.e., 5.98 m (235.50 in.) above Level 0, or 5.00 m (196.44 in.) above TAF.
22.0	Suppression pool water average temperature rises to 35.13°C (95.24°F) in response to the first S/RV pops.
29.0	All 4 S/RVs are completely closed.
29.7	Two out of 13 S/RVs start to open.

ACTIVITIES RELATED TO TASK 2

- INSIGHTS GAINED FROM RESULTS OF PUBLISHED PRA ASSESSMENTS OF STATION BLACKOUT

TASK 2 SUMMARY

				←STATION BLACKOUT→	
STUDY	PLANT	DOMINANT BLACKOUT SEQUENCES	HIGH RISK CONT'T. FAILURE MODES	APPROX. % AGE OF TOTAL CORE DAMAGE PROB.	APPROX. % AGE OF TOTAL RISK
IREP	CRYSTAL RIVER-3	TML_1B_1	OVERPRESSURE	15%	15%
RSS	SURRY	TML_1B_1	OVERPRESSURE, HYDROGEN BURN	15%	30%
RSSMAP	SEQUOYAH	TML_1B_1	OVERPRESSURE, HYDROGEN BURN	1%	1%
RSSMAP	OCONEE	TML_1B_1	HYDROGEN BURN	3%	3%
INDUSTRY	ZION	TML_1B_1	OVERPRESSURE	1%	3%
RSS	PEACH BOTTOM-2,3	TMB_3, TMU_1B_1	OVERPRESSURE	1%	1%
RSSMAP	GRAND GULF	TMB_3, TMU_1B_1, TMQ_1B_3	OVERPRESSURE	3%	3%
INDUSTRY	LIMERICK	TMU_2B_2	OVERPRESSURE	25%	25%
INDUSTRY	BIG ROCK POINT	TMU_1B_1, TMQ_1B_1	ISOLATION FAILURE	1%	1%

CONCLUSIONS DRAWN FROM PUBLISHED PRA ASSESSMENTS

PWRs:

SEQUENCE OF MOST IMPORTANCE TO BLACKOUT IDENTIFIED AS EARLY FAILURE OF AFWS & SUBSEQUENT FAILURE TO RECOVER AC POWER

SIGNIFICANT CONTAINMENT FAILURE MODES IDENTIFIED AS OVERPRESSURE, HYDROGEN BURN

BLACKOUT CONTRIBUTION TO RISK UNCLEAR

BWRs:

SEQUENCE OF MOST IMPORTANCE TO BLACKOUT NOT CLEAR

SIGNIFICANT CONTAINMENT FAILURE MODE IDENTIFIED AS OVERPRESSURE

BLACKOUT CONTRIBUTION TO RISK UNCLEAR

ACTIVITIES RELATED TO TASK 3

SCOPE OF PLANT FEATURES REVIEWED FOR DETERMINING SHUTDOWN COOLING RELIABILITY UNDER STATION BLACKOUT

SYSTEM INFORMATION & INTERACTIONS COVERED IN THE ABOVE REVIEW

EXTENT OF INFORMATION SOURCES USED FOR THIS REVIEW

EXAMPLES OF INFORMATION OBTAINED

OTHER IMPORTANT INSIGHTS GAINED DURING PERFORMANCE OF TASK 3

PLANT FEATURES REVIEWED

DECAY HEAT REMOVAL & RCS MAKEUP SYSTEMS

SUPPORT SYSTEMS FOR THE ABOVE

SYSTEMS/COMPONENTS AFFECTING RCS INTEGRITY UNDER STATION BLACKOUT

CONTAINMENT SYSTEMS

CONTROL ROOM INDICATIONS & SYSTEM CONTROL CAPABILITY

PROCEDURES & HUMAN ACTIONS

FIGURE B-1

SYSTEM INFORMATION & INTERACTIONS
COVERED IN REVIEW OF
AC-INDEPENDENT SYSTEMS

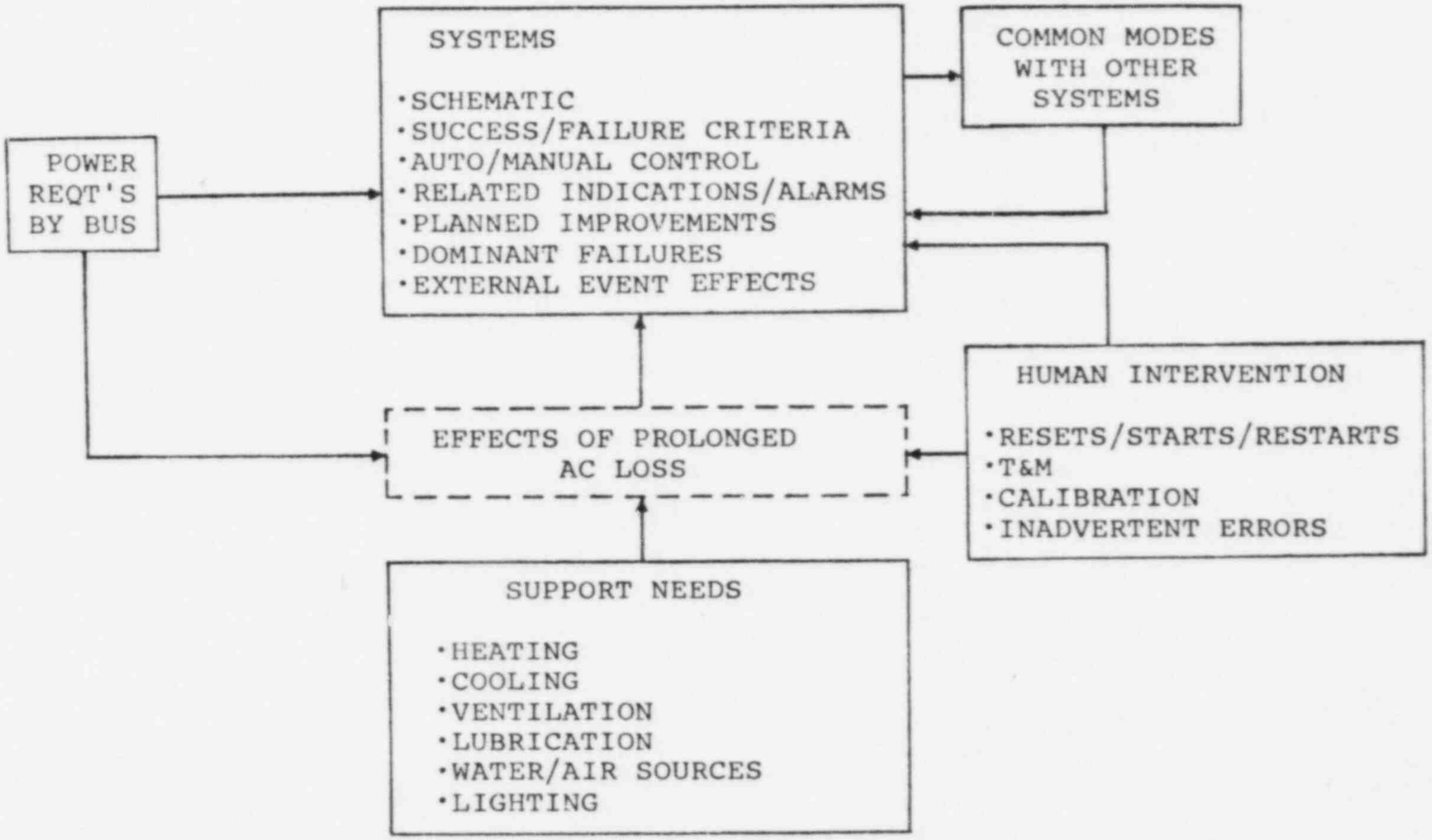


FIGURE B-2

SYSTEM INFORMATION & INTERACTIONS COVERED IN REVIEW OF AC-DEPENDENT SYSTEMS

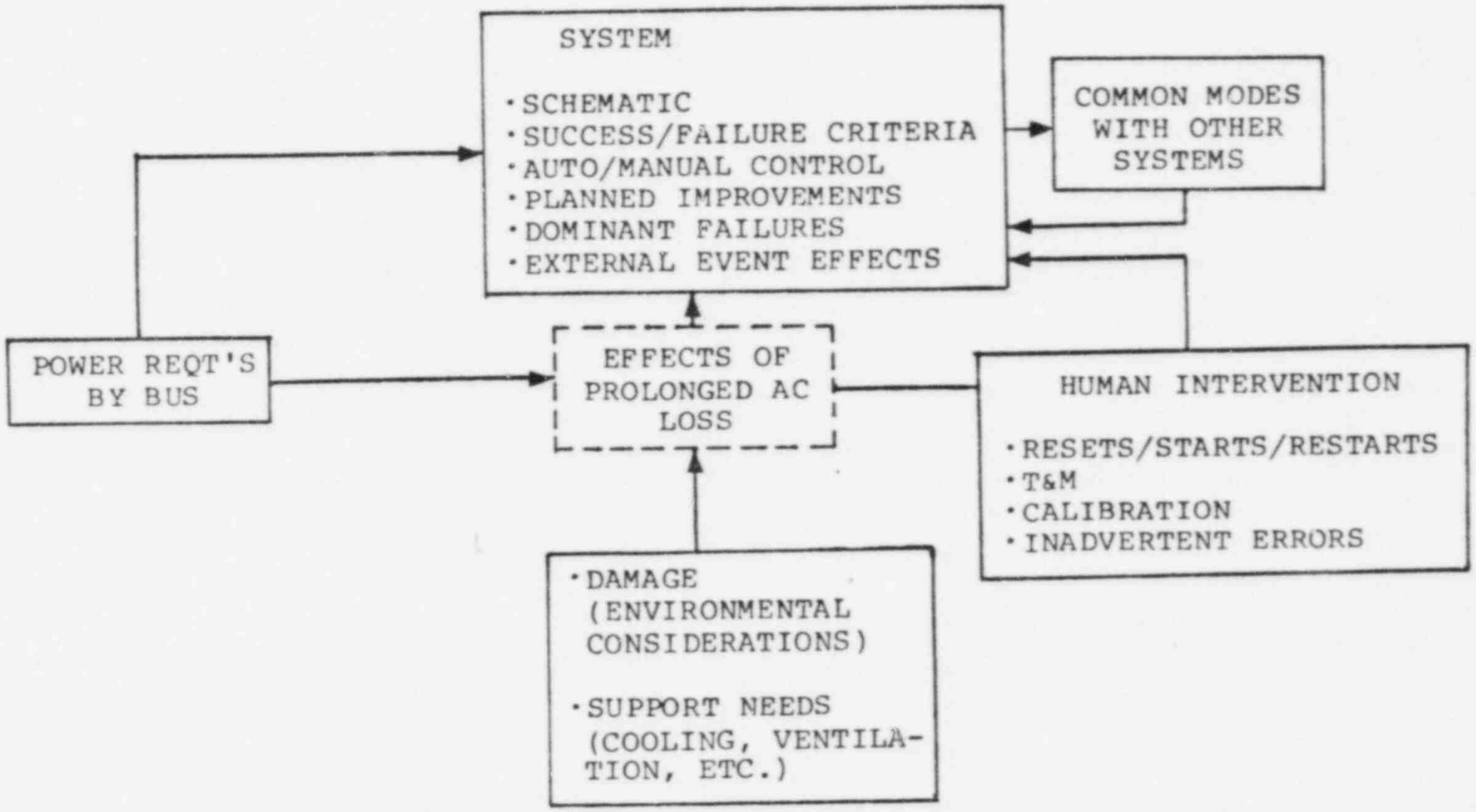


Table B-1

SUMMARY OF INFORMATION SOURCES

SOURCE / TYPE OF INFORMATION	FSAR's	PRA's	SASA	GENERIC FEED-WATER STUDIES	NUREG-0737 RESPONSE	INDUSTRY B&W AFW RESPONSE	S.B. PROCEDURES NRC LETTER 81-04	NRC LER DATA SUMMARIES	SWAIN'S HANDBOOK HUMAN FACTOR	LERS	DC POWER STUDY	PLANT VISITS	MISC.	NRC PLANT DATA FILE
SYSTEM INFORMATION	x	x		x	x	x	x					x	x	x
SYSTEM SUCCESS CRITERIA	x	x	x	x		x								
SYSTEM/ COMPONENT FAILURE MODES		x	x	x	x	x		x		x	x		x	
OPERATING PROCEDURES	x	x		x		x	x					x		
FAILURE DATA		x		X	x			x	x	x	x		x	
TIMING OF EVENTS IN ACCIDENT SEQUENCE	x	x	x	x	X		X					X		

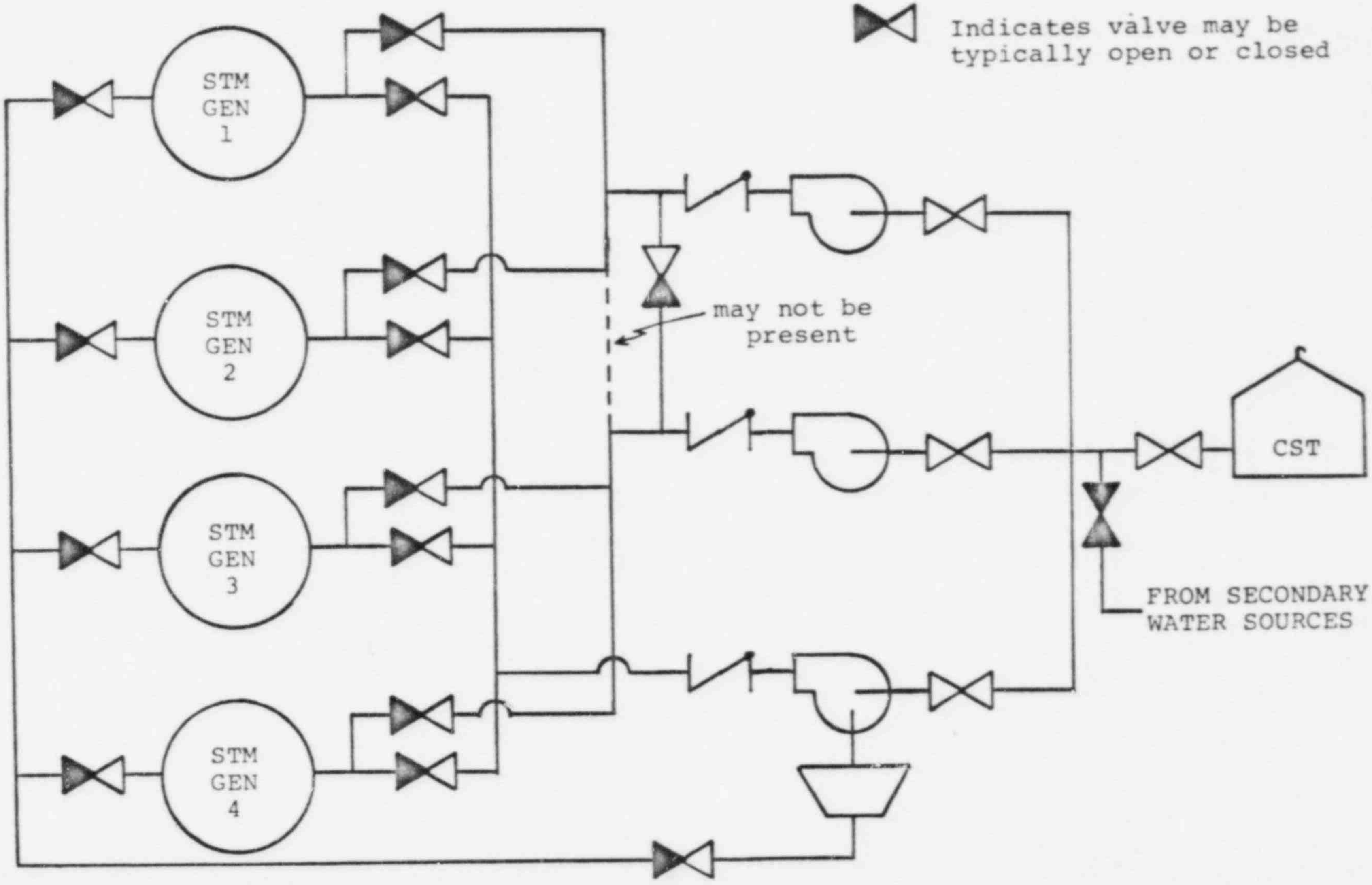


FIGURE B-4. SIMPLIFIED DIAGRAM OF TYPICAL AUXILIARY FEEDWATER SYSTEM

IMPORTANT FEATURES OF AFWS IN PWRs

TURBINE TRAIN:

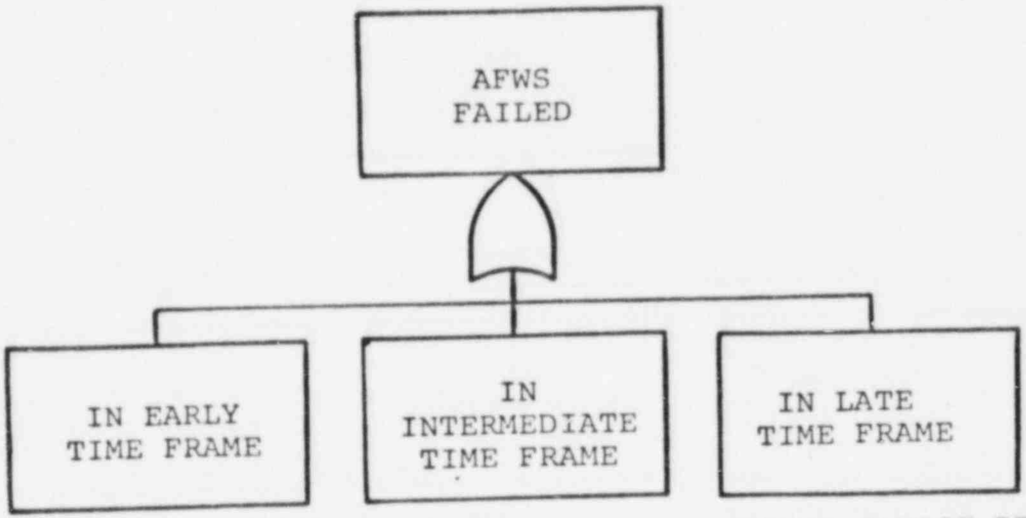
- USUALLY 1 TRAIN BUT AS MANY AS 3
- USUALLY POWERED BY STATION BATTERIES BUT MAY HAVE DEDICATED BATTERY
- ON LOSS OF DC POWER, MAY OR MAY NOT BE MANUALLY CONTROLLABLE
- ALL ARE OR WILL BE AC-INDEP., HAVE LOCKED OPEN VALVES WHERE POSSIBLE, & START AUTOMATICALLY (TMI FIX)

MOTOR TRAIN:

- USUALLY 1 OR 2 TRAINS BUT 0 TRAINS ON SOME PLANTS WITH MULTIPLE TURBINE TRAINS
- USUALLY POWERED BY PLANT AC/DC BUT MAY HAVE DEDICATED DIESEL AND BATTERY SYSTEM

CST (AFWS WATER SOURCE) LASTS 6 TO >24 HRS.

SECONDARY AFWS WATER SOURCE MAY REQUIRE AC POWER & RECONFIGURATION TO SECONDARY SOURCE MAY BE MANUAL OR AUTOMATIC



- TURBINE HARDWARE/ T&M
- VALVE HARDWARE
- EARLY DC POWER FAILURE & AC NOT RESTORED

- DC POWER DEPLETION OR FAILURE DUE TO HI TEMP & AC NOT RESTORED

- WATER SOURCE DEPLETED & (1) OPERATOR FAILS TO RECONFIGURE OR (2) SECONDARY SOURCE IS AC-DEPENDENT & AC NOT RESTORED

FIGURE B-5. AFWS MAJOR FAULT MODES

OTHER POTENTIALLY IMPORTANT INSIGHTS FROM TASK 3

PROCEDURES SHOULD BE DETAILED FOR BRINGING PLANT TO A SAFE SHUTDOWN EVEN ONCE AC POWER IS RESTORED

THUS FAR, STATION BLACKOUT PROCEDURES VARY CONSIDERABLY

EXTERNAL EVENTS (SEISMIC,FIRE,WIND) COULD CAUSE STATION BLACKOUT OR CONDITIONS SIMILAR TO BLACKOUT WITH FREQUENCIES OF 1E-4 TO LESS THAN 1E-6

CHECK TO ENSURE SECURITY SYSTEMS DO NOT PREVENT ROOM ACCESS UNDER LOSS OF AC/DC POWER

THERMAL SHOCK: ASSUMED IF COOLING RESTORED BEFORE SIGNIFICANT CORE DAMAGE, ANY RESULTING THERMAL SHOCK WILL NOT RESULT IN FAILURE OF LARGE MAGNITUDE

TWO PHASE FLOW(PWR): SASA ANALYSES & TMI SHOW THAT TWO PHASE FLOW WILL OCCUR BEFORE CORE UNCOVERY BUT IS REVERSIBLE

DOWNTIME DUE TO TEST & MAINTENANCE MAY BE ABNORMALLY HIGH ON SOME AC-INDEP. HEAT REMOVAL SYSTEMS

EXTERNAL EVENTS

- DEPENDS ON PLANT SITE AND PLANT DESIGN

EVENT	PLANT "WEAKNESSES"
SEISMIC	SWITCHYARD,CONTROL,NON-SEISMIC
FIRE	AREAS WITH MULTIPLE DIVISIONS
WIND	GRID TOWERS,SWITCHYARD,TALL STRUCTURES
FLOOD	AREAS WITH MULTIPLE DIVISIONS

- CORE DAMAGE PROBABILITY FOR ALL ABOVE: E-4 -<E-6
- OTHER EVENTS:VOLCANO,TOXIC GASES,AIR CRASHES...
  APPEAR LESS LIKELY

ACTIVITIES RELATED TO TASKS 4&5 ("RESULTS" TASKS)

"TYPICAL" FAULT TREE DEVELOPMENT DEFINING SYSTEM FAILURE MODES

SOURCES OF FAILURE DATA, BLACKOUT LIKELIHOOD, & AC RECOVERY PROBABILITIES

POST-TMI CHANGES FACTORED IN TO SEQUENCE ANALYSES

BASIC DESCRIPTIONS OF 4 BASE CASE ANALYSES

ACCIDENT SEQUENCE RESULTS OF 4 BASE CASE ANALYSES

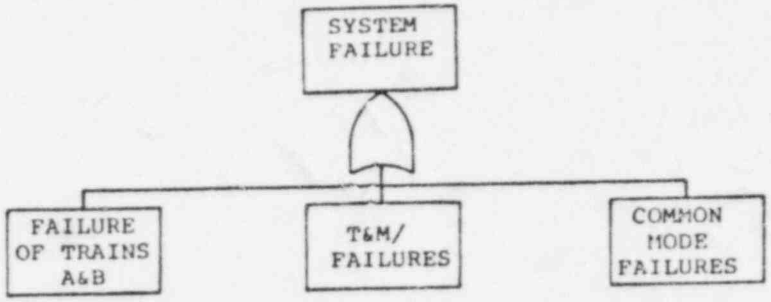
COMPARISON OF ABOVE RESULTS WITH PROPOSED CORE MELT SAFETY GOAL

IMPORTANT SENSITIVITIES COVERING OTHER PLANT CONFIGURATIONS & "OPTIONS" FOR REDUCING THE RISK FROM STATION BLACKOUT

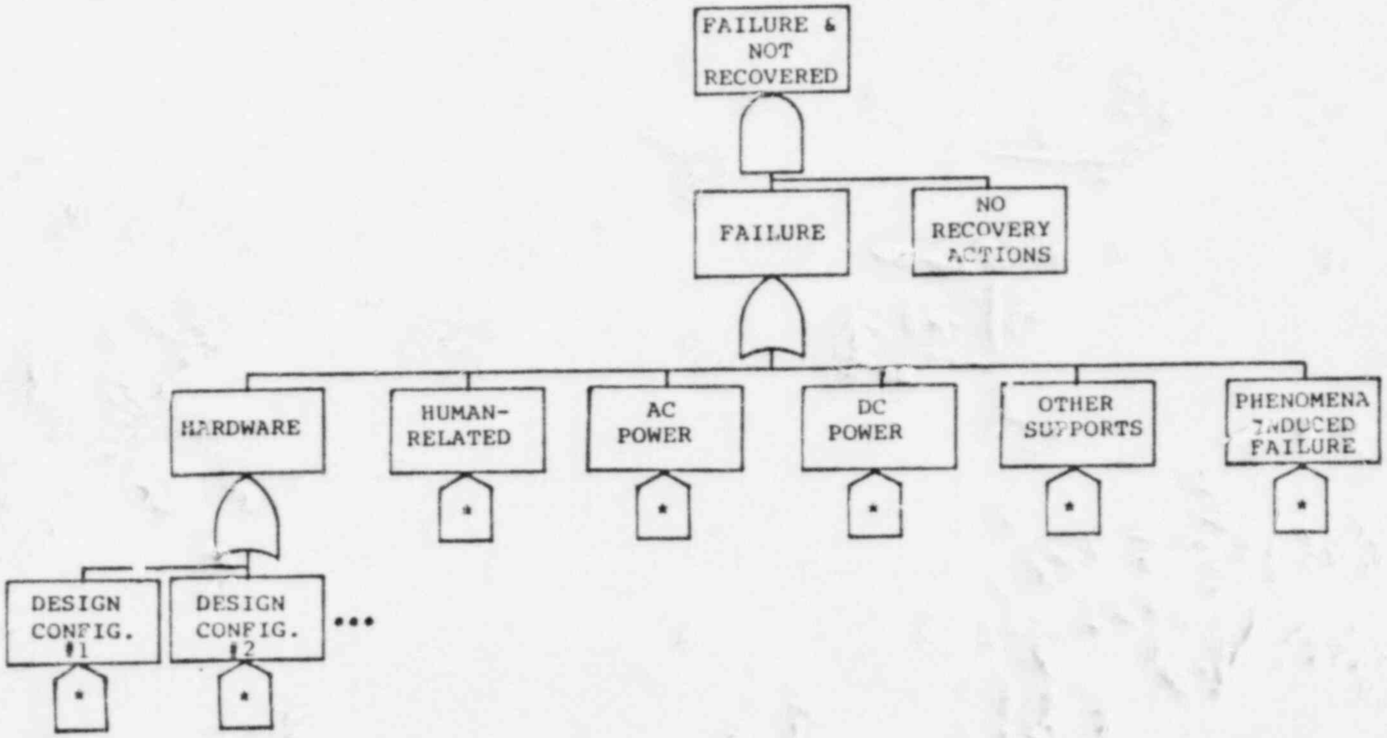
CONTAINMENT FAILURE INSIGHTS TO ADD RISK PERSPECTIVES

TYPICAL DETAILED FAULT TREE STRUCTURE

OVERALL TOP LOGIC:



FAILURES TYPICALLY DEPICTED AS:



*Turn "on" and "off" to select design variations and to introduce failure modes at specific times following the initiating event.

DATA SOURCES

- SYSTEM/COMPONENT/HUMAN FAILURE DATA (BASED ON PREVIOUS ASSESSMENTS)
  - 10 PRAs & ONGOING IREP ANALYSES
  - NRC GENERIC FEEDWATER STUDIES
  - NUREG 0737 RESPONSES
  - NRC LER DATA SUMMARIES
  - LER REVIEW
  - DC POWER STUDY
  - "SWAIN HANDBOOK"
  - MISC. LETTERS & REPORTS
- CRITICALLY REVIEWED FOR CURRENT APPLICABILITY
- "REPRESENTATIVE" GENERIC VALUES USED FOR BASE CASE ANALYSES
- HUMAN ERRORS INVOLVING RECOVERY ACTIONS
  - ■ RANGE IN STUDY FROM 0.5 TO 1E-3
    - A:- 0.5:
      - SHORT TIME AVAILABLE &/OR UNUSUAL PRACTICE OR NOT IN PROCEDURES
      - DESIGN LIMITATION
    - B:-1E-1 TO MID E-2: EARLY FAILURES WITH NON-ROUTINE RECOVERY STEPS
    - C:-MID E-2 TO MID E-3: EARLY FAILURES BUT ROUTINE RECOVERY STEPS
    - D:- 1E-3: LATE FAILURES WITH AMPLE TIME FOR RECOVERY
  - ■ ALL ERROR FACTORS=10 EXCEPT FOR 0.5(2)
- BLACKOUT LIKELIHOOD & AC RECOVERY POTENTIAL FROM ORNL

POST-TMI CHANGES
FACTORED IN TO BASE CASE ANALYSES

TMI FIXES CONCERNING AFWS

RCIC RESTARTS MADE AUTOMATIC

REDUCTION IN RELIEF VALVE DEMANDS

ADEQUATE INDICATION, ALARM STATUS, & CONTROL CAPABILITY

STATION BLACKOUT PROCEDURES BEING WRITTEN

PWR GENERIC PLANT CLASS DESCRIPTION
(FOR BASE CASE ANALYSIS)

2 DIVISIONS OF SDC SYSTEMS

2 DIVISIONS OF EMERGENCY POWER

COMMON SERVICE WATER DEPENDENCY FOR COOLING OF DGs & AC PUMPS

BATTERY DEPLETION IN 5 HRS.

1 STEAM TRAIN OF AFWS

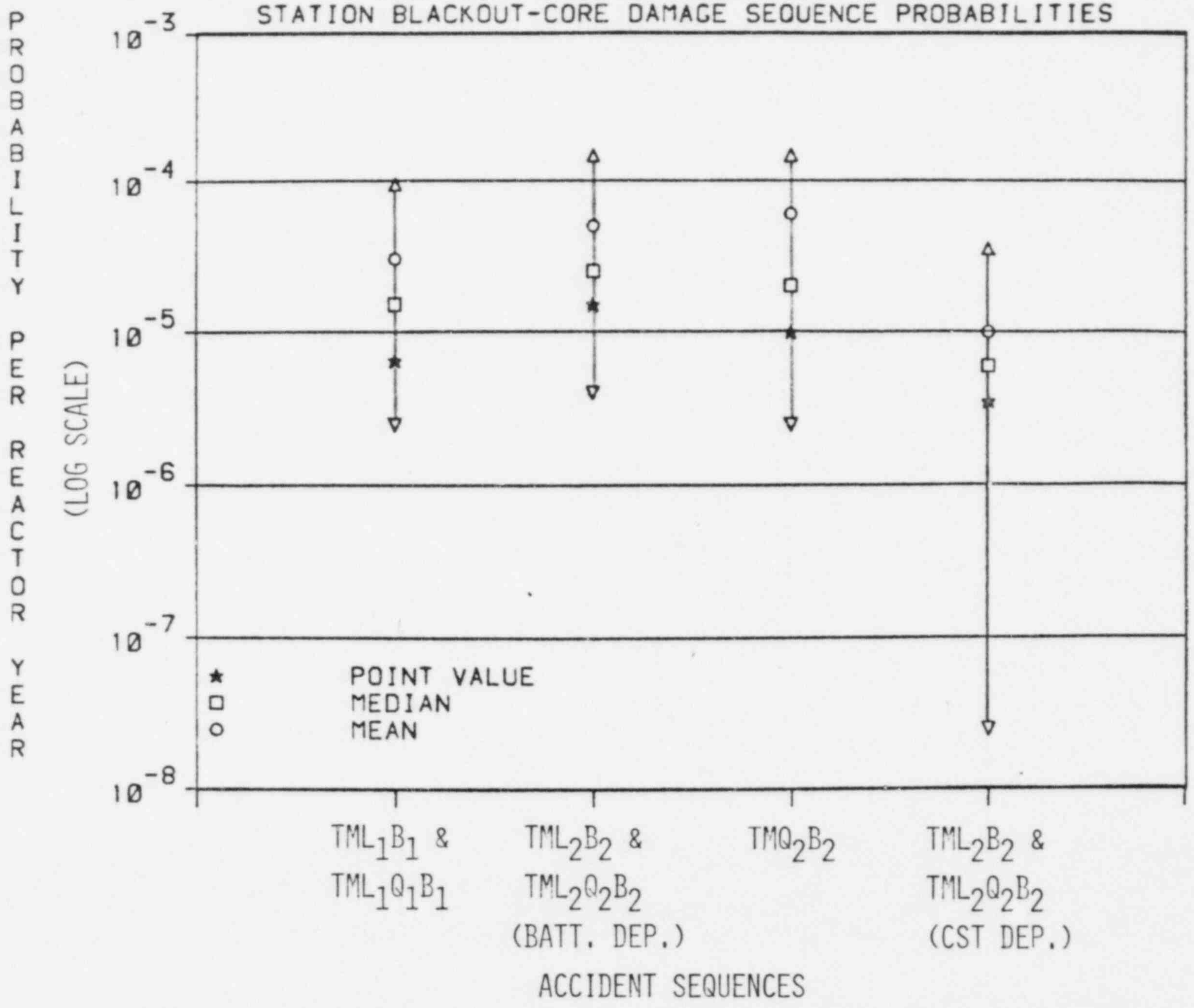
0.5 PROBAB. OF AFWS SUCCESS AFTER BATTERY DEPLETION

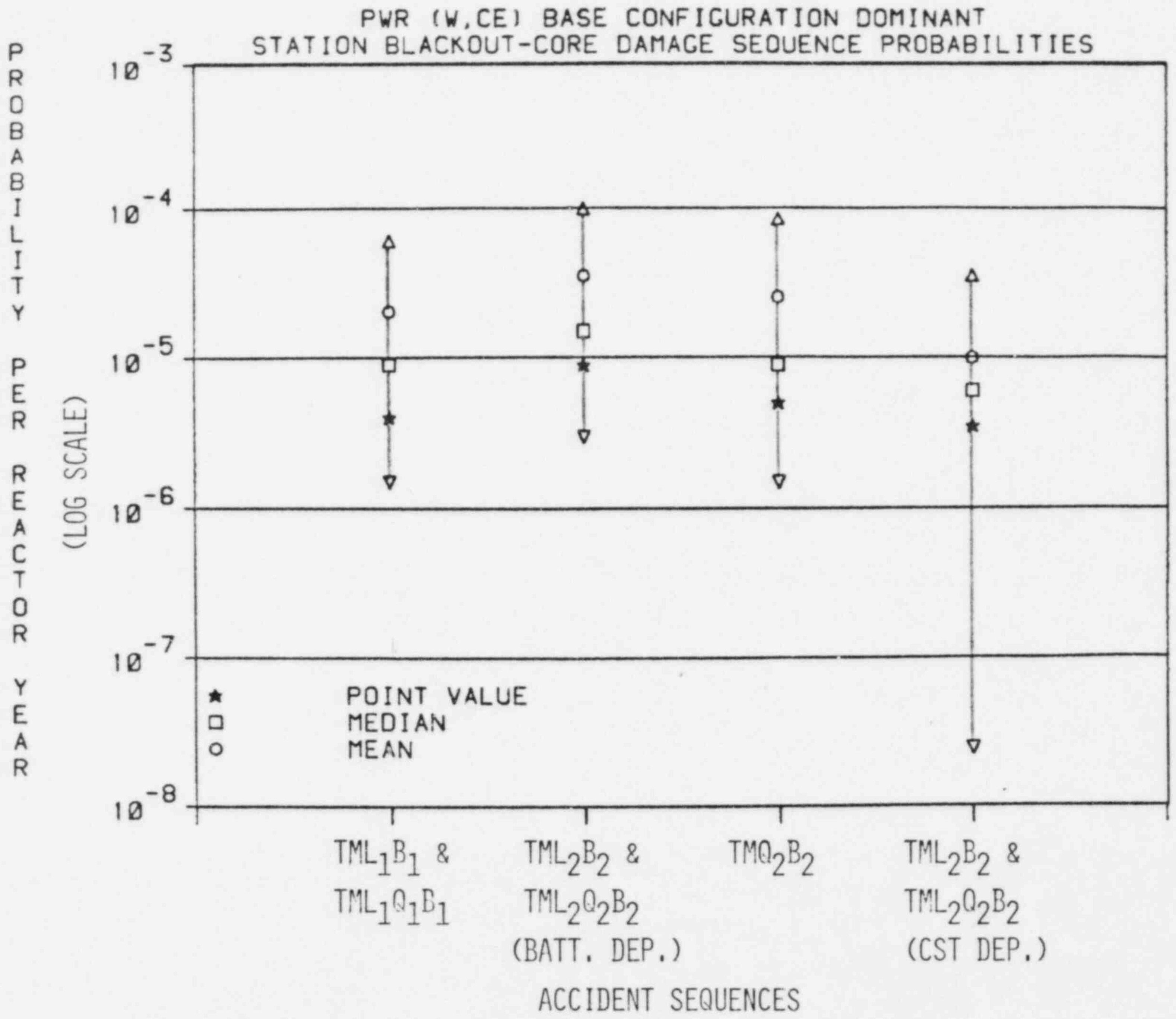
0.5 PROBAB. THAT RCS PUMP SEAL FAILURE SUFFICIENT TO UNCOVER CORE IN 8-12 HRS.

CST DEPLETED IN 8 HRS.

AC DEPENDENCY IN ALTERNATE WATER SOURCE

PWR (B&W) BASE CONFIGURATION DOMINANT
STATION BLACKOUT-CORE DAMAGE SEQUENCE PROBABILITIES





PWR GENERIC PLANT CLASS
DOMINANT ACCIDENT SEQUENCES

SEQUENCES	MEAN PROB./RY	MAJOR FACTORS AFFECTING SEQUENCE PROBAB.
TML1B1 & TML1Q1B1	3.0-2.0 E-5	AFWS STM TRAIN UNAVAIL. AC RECOVERY,AC FOR RCS ISOLATION
TML2B2 & TML2Q2B2 (BATT DEP.)	5.0-3.5 E-5	AFWS-DC-OPER INTERACTION, AC RECOVERY
TMQ2B2	6.0-2.5 E-5	LARGE PUMP SEAL FAILURE,AC RECOVERY,COMMON SW DEPENDENCIES
TML2B2 & TML2Q2B2 (CST DEP.)	1.0 E-5	CST DEP. TIME,AC RECOVERY, AC/DC DEPENDENCIES IN ALT. WATER SOURCE

PWR SENSITIVITY EXAMPLES

ITEM	VALUE USED	SENSITIVITY	POINT ESTIMATE EFFECTS		
			SEQUENCE	BEFORE	AFTER
AFWS STM TRAIN UNAVAIL.	4E-2	1.2E-1, 4E-3	TML_1B_1	6.5-4.0E-6	2.0-1.2E-5 6.5-4.0E-7
			ΣCD	3.5-2.0E-5	5.0-3.0E-5 3.0-1.5E-5
AFWS 2 STM TRAINS	-	5E-4	TML_1B_1	6.5-4.0E-6	6.5-4.0E-7
			ΣCD	3.5-2.0E-5	3.0-1.5E-5
AFWS 1 STM TRAIN AND DED. INDEP. DIESEL/DC TRAIN	-	1E-2	TML_1B_1	6.5-4.0E-6	NEGL.
			TML_2B_2 (BATT. DEP.)	1.5-0.9E-5	NEGL.
			TML_2B_2 (CST DEP.)	3.5E-6	7.0E-6
			ΣCD	3.5-2.0E-5	1.5-1.0E-5

PWR SENSITIVITY EXAMPLES

ITEM	VALUE USED	SENSITIVITY	POINT ESTIMATE EFFECTS		
			SEQUENCE	BEFORE	AFTER
OPERATOR FAILS TO RUN AFWS W/O DC	0.5	1.0, 0.1	TML_2B_2 (BATT. DEP.)	1.5-0.9E-5	3.0-2.0E-5 3.0-2.0E-6
			TMQ_2B_2 (B&W ONLY)	1.0E-5	5.0E-6 1.5E-5
			TML_2B_2 (CST DEP.)	3.5E-6	NEGL. 7E-6
			ΣCD	3.5-2.0E-5	4.0-2.5E-5 3.0-2.0E-5

PWR SENSITIVITY EXAMPLES

ITEM	VALUE USED	SENSITIVITY	POINT ESTIMATE EFFECTS		
			SEQUENCE	BEFORE	AFTER
COMMON SW DEPENDENCIES	8E-5	NEGL.	TML_1B_1	6.5-4.0E-6	5.0-3.0E-6
			TML_2B_2 (BATT. DEP.)	1.5-0.9E-5	1.0-0.7E-5
			TMQ_2B_2	1.0-0.5E-5	5.0E-6 TO NEGL.
			TML_2B_2 (CST DEP.)	3.5E-6	3.0E-6
			ΣCD	3.5-2.0E-5	3.0-1.5E-5

PWR SENSITIVITY EXAMPLES

ITEM	VALUE USED	SENSITIVITY	POINT ESTIMATE EFFECTS		
			SEQUENCE	BEFORE	AFTER
BATTERY DEPLETION TIME	5 HRS.	2 HRS., 12 HRS.	TML_2B_2 (BATT. DEP.)	1.5-0.9E-5	3.0-2.0E-5 3.0-2.0E-6
			TMQ_2B_2 (B&W ONLY)	1.0E-5	1.5E-5 6.0E-6
			TML_2B_2 (CST DEP.) -12 HR. ONLY-	3.5E-6	7.0E-6
			ΣCD	3.5-2.0E-5	5.5-3.0E-5 2.0E-5
SEAL LEAK TIME	0.5@	1.0@	TMQ_2B_2	1.0-0.5E-5	4.5-1.5E-5
	8-12 HRS.	2 HRS.	ΣCD	3.5-2.0E-5	7.0-3.0E-5
BLACKOUT PROBABILITY	2E-4	2E-3, 1E-5	ΣCD	3.5-2.0E-5	3.5-2.0E-4 2.0-1.0E-6
AFWS, BATT. DEP. TIME, SEAL LEAK TIME, CST DEP. TIME	4E-2, 5 HRS.	4E-3, 12 HRS.	TML_1B_1	6.5-4.0E-6	6.5-4.0E-7
	0.5@ 8-12 HRS. 8 HRS.	1 DAY, 1 DAY	TML_2B_2 (BATT. DEP.)	1.5-0.9E-5	3.0-2.0E-6
			TMQ_2B_2	1.0-0.5E-5	NEGL.
			TML_2B_2 (CST DEP.)	3.5E-6	NEGL.
			ΣCD	3.5-2.0E-5	3.5-2.5E-6

BWR w/ISOLATION CONDENSER(S)
GENERIC PLANT CLASS DESCRIPTION
(FOR BASE CASE ANALYSIS)

A. 2 DIVISIONS OF SDC SYSTEMS

2 DIVISIONS OF EMERGENCY POWER

COMMON SERVICE WATER DEPENDENCY FOR COOLING OF DGs & AC PUMPS

BATTERY DEPLETION IN 5 HRS.

2 CONDENSERS USING DC VALVES & 1 FIREPUMP (DEDICATED DIESEL) FOR SHELL SIDE MAKEUP

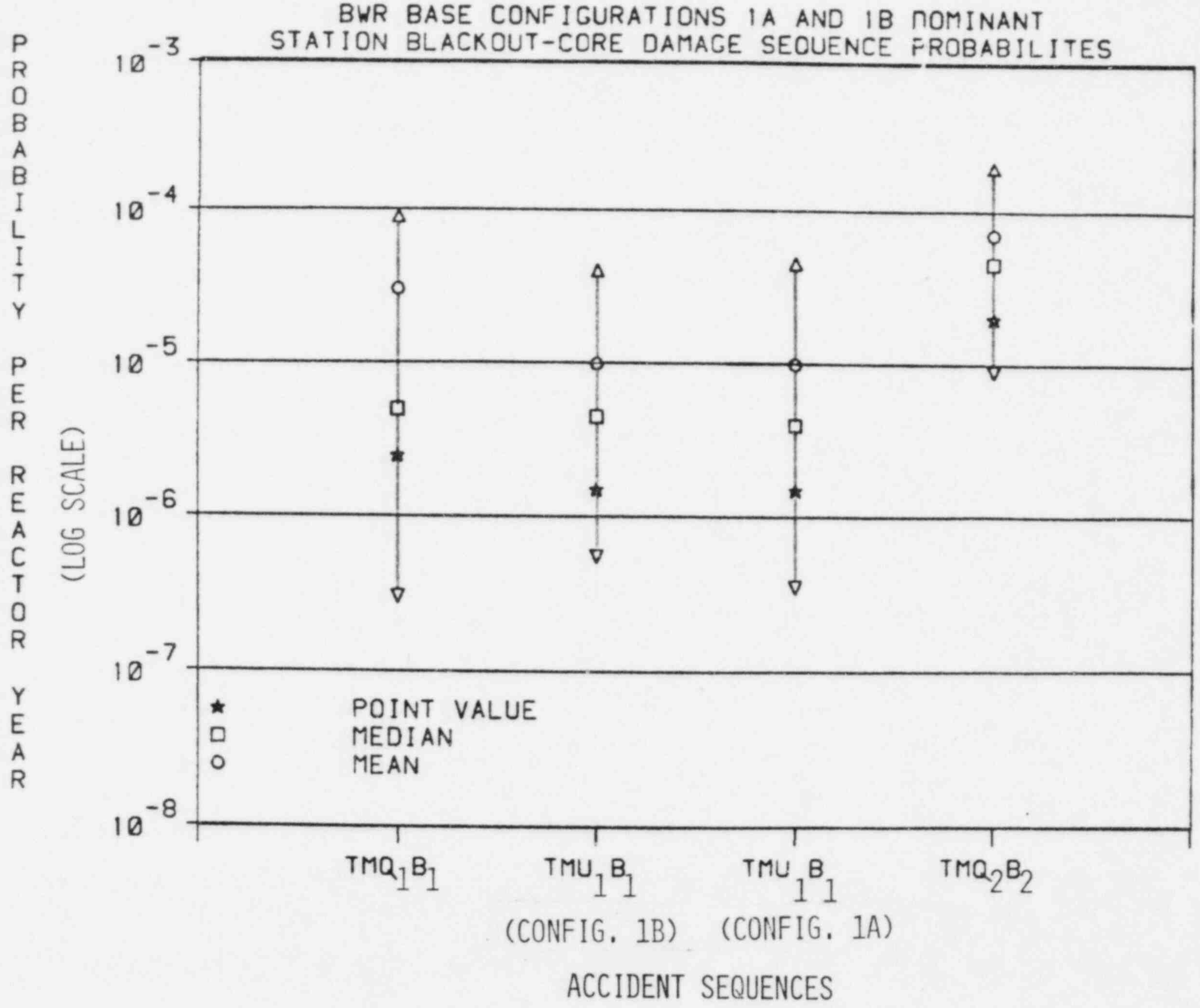
AC VALVES IN SHELL SIDE MAKEUP LINES (5E-3 FAILURE TO MANUALLY OPEN)

NO AC-INDEPENDENT RCS MAKEUP

1 SRV DEMAND

RCS PUMP SEAL FAILURE SUFFICIENT TO UNCOVER CORE IN 12 HRS.

B. AS ABOVE EXCEPT: 1 CONDENSER
AUTO FWCI SYSTEM FOR RCS MAKEUP



BWR BASE CONFIGURATIONS 1A AND 1B DOMINANT STATION BLACKOUT-CORE DAMAGE SEQUENCE PROBABILITES

BWR w/ISO COND GENERIC PLANT CLASS DOMINANT ACCIDENT SEQUENCES

SEQUENCE	MEAN PROB./RY	MAJOR FACTORS AFFECTING SEQUENCE PROBAB.
TMQ1B1	2.0 E-5	STUCK-OPEN SRV,AC RECOVERY
TMU1B1	1.0 E-5	COND. UNAVAIL.,AC RECOVERY
TMQ2B2	7.0 E-5	LARGE PUMP SEAL FAILURE, AC RECOVERY,COMMON SW DEPENDENCIES

BWR W/ISOLATION CONDENSER SENSITIVITY EXAMPLES

ITEM	VALUE USED	SENSITIVITY	POINT ESTIMATE EFFECTS		
			SEQUENCE	BEFORE	AFTER
OPERATOR FAILURE TO INITIATE	5E-3	5E-2, 1E-3	TMU_1B_1	1.5E-6	6.0E-6 1.0E-6
			ΣCD	2.5E-5	3.0E-5 2.5E-5
ADD FIREPUMP FOR RCS MAKEUP	--	5E-2	ΣCD	2.5E-5	1.5E-6
BLACKOUT PROBABILITY	2E-4	2E-3, 1E-5	ΣCD	2.5E-5	2.5E-4 1.5E-6
OFFSITE NON-RECOVERY	SEE REPORT	3↑, 3↓	TMU_1B_1	1.5E-6	4.5E-6 5.0E-7
			TMQ_2B_2	2.0E-5	6.0E-5 7.0E-6
			ΣCD	2.5E-5	6.5E-5 1.0E-5

BWR w/HPCI-RCIC GENERIC PLANT CLASS DESCRIPTION (FOR BASE CASE ANALYSIS)

2 DIVISIONS OF SDC SYSTEMS

2 DIVISIONS OF EMERGENCY POWER

COMMON SERVICE WATER DEPENDENCY FOR COOLING OF DGs & AC PUMPS & HPCI/RCIC PUMP ROOMS

BATTERY DEPLETION IN 5 HRS.

0.5 PROBAB. OF RCIC SUCCESS AFTER BATTERY DEPLETION

NEGLIG. PROBAB. OF HPCI SUCCESS AFTER BATTERY DEPLETION

RCIC THROTTLED; HPCI NOT THROTTLED

HPCI/RCIC ISOLATE BY 5 HOURS DUE TO HI ROOM TEMP.

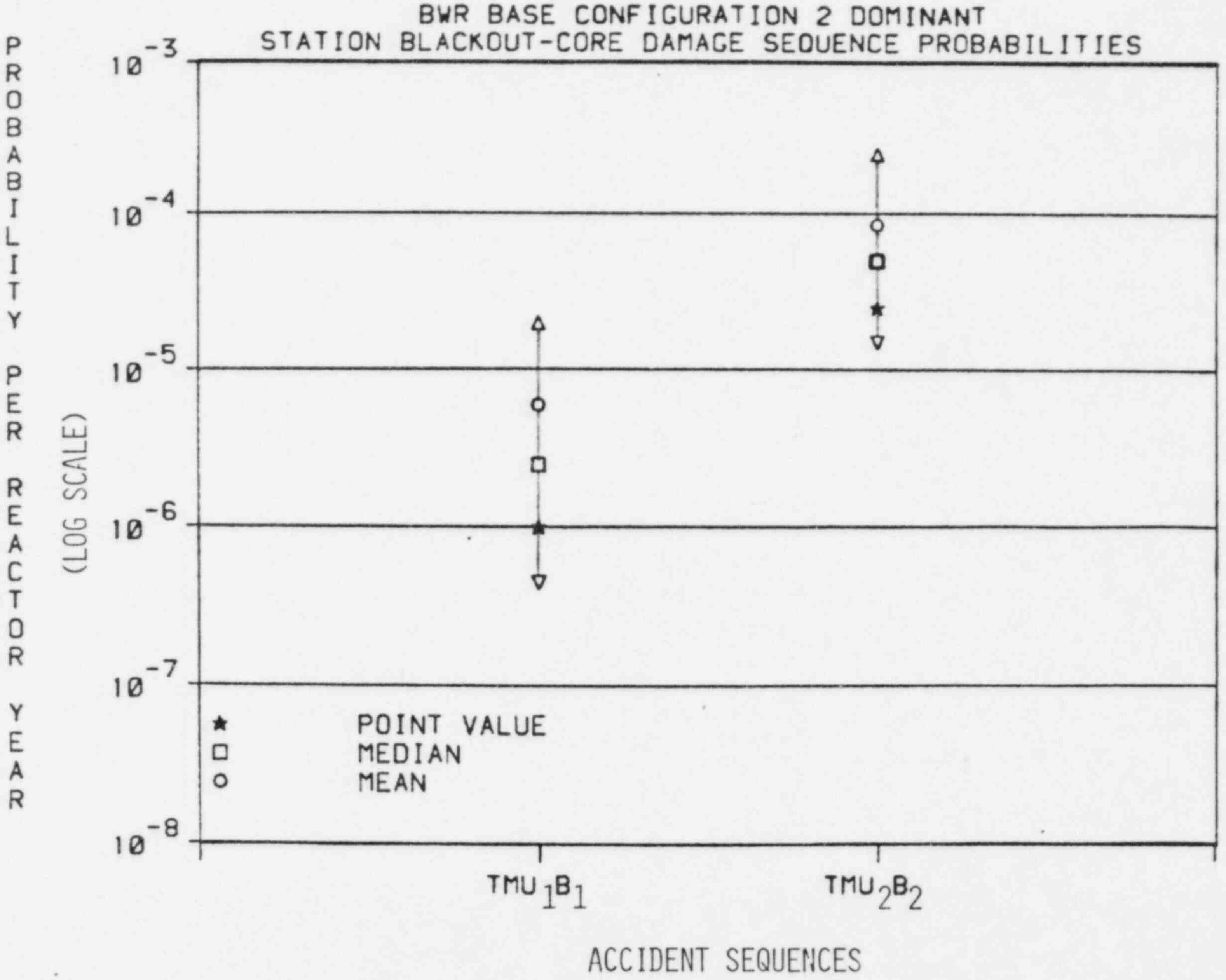
HPCI/RCIC FAIL DUE TO HI TEMP BY 8 HOURS

HPCI/RCIC FAIL (0.1,0.05) DUE TO LOW STEAM PRESS 5-6 HRS.

HPCI/RCIC CAN HANDLE RCS PUMP SEAL LEAK OR OPEN SRV

CST DEPLETED IN 8 HRS.

TRANSFER TO SUPP. POOL NOT MADE TIL AT OR FOLLOWING BATTERY DEPLETION



BWR BASE CONFIGURATION 2 DOMINANT
STATION BLACKOUT-CORE DAMAGE SEQUENCE PROBABILITIES

BWR w/HPCI–RCIC GENERIC PLANT CLASS DOMINANT ACCIDENT SEQUENCES

SEQUENCE	MEAN PROB./RY	MAJOR FACTORS AFFECTING SEQUENCE PROBAB.
TMU1B1	6.0 E–6	HPCI/RCIC UNAVAIL.AC RECOVERY
TMU2B2	8.5 E–5	HPCI/RCIC–DC/VENTIL/OPER INTERACTIONS,AC RECOVERY, COMMON SW DEPENDENCIES

BWR W/HPCI-RCIC SENSITIVITY EXAMPLES

ITEM	VALUE USED	SENSITIVITY	POINT ESTIMATE EFFECTS		
			SEQUENCE	BEFORE	AFTER
OPERATOR FAILS TO RUN HPCI-RCIC W/O DC/ VENTILATION	0.5	1.0, 0.1	TMU_2B_2	2.5E-5	3.0E-5 2.0E-5
			ΣCD	2.5E-5	3.0E-5 2.0E-5
HPCI-RCIC RUNS W/O VENTILATION	5-8 HRS.	12 HRS.	TMU_2B_2	2.5E-5	1.0E-5
			ΣCD	2.5E-5	1.0E-5
BLACKOUT PROBABILITY	2E-4	2E-3, 1E-5	ΣCD	2.5E-5	2.5E-4 1.5E-6

BWR w/HPCS-RCIC GENERIC PLANT
CLASS DESCRIPTION
(FOR BASE CASE ANALYSIS)

2 DIVISIONS OF SDC SYSTEMS & EMERGENCY POWER

COMMON SERVICE WATER DEPENDENCY FOR COOLING OF DGs & AC PUMPS (EXCEPT HPCS) & RCIC PUMP ROOM

BATTERY DEPLETION IN 5 HRS.

HPCS HAS DEDICATED DG, DC, SERVICE WATER

0.5 PROBAB. OF RCIC SUCCESS AFTER BATTERY DEPLETION

RCIC THROTTLED, HPCS NOT THROTTLED

RCIC ISOLATES BY 5 HRS & FAILS BY 8 HRS DUE TO HI RM TEMP

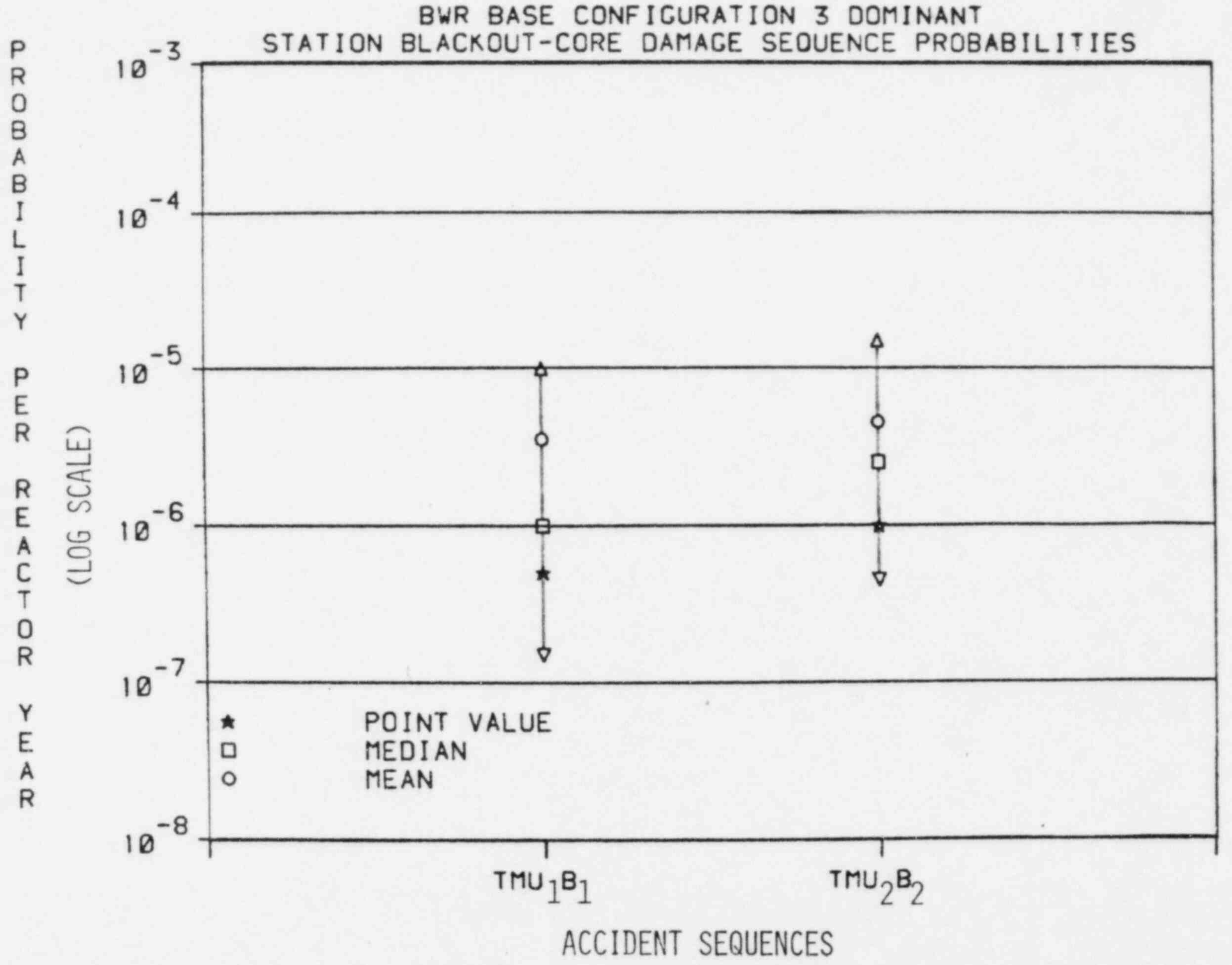
RCIC FAILS (0.05) DUE TO LOW STEAM PRESS IN 5-6 HRS.

HPCS REQUIRES PERIODIC START & STOP OPERATION

HPCS/RCIC CAN HANDLE RCS PUMP SEAL LEAK OR OPEN SRV

CST DEPLETED IN 8 HRS.

TRANSFER TO SUPP. POOL NOT MADE TIL AT OR FOLLOWING BATTERY DEPLETION



BWR BASE CONFIGURATION 3 DOMINANT STATION BLACKOUT-CORE DAMAGE SEQUENCE PROBABILITIES

BWR w/HPCS-RCIC GENERIC PLANT CLASS DOMINANT ACCIDENT SEQUENCES

SEQUENCE	MEAN PROB./RY	MAJOR FACTORS AFFECTING SEQUENCE PROBAB.
TMU1B1	3.5 E-6	HPCS/RCIC UNAVAIL,AC RECOVERY
TMU2B2	4.5 E-6	HPCS UNAVAIL,RCIC-DC/VENTIL/ OPER INTERACTIONS, AC RECOVERY

STATION BLACKOUT
& LOSS OF INSTRUMENTATION

SUSCEPTIBLE DESIGN: 2 INVERTERS
AC IS PREFERRED SOURCE
MECHANICAL SWITCHOVER

FREQUENCY OF OCCURRENCE: ~1E-5

CORE DAMAGE PROBABILITY: $\lesssim$1E-7

COMPARISON OF CORE DAMAGE PROBABILITY PER REACTOR YEAR DUE TO STATION BLACKOUT WITH TOTAL CORE MELT SAFETY GOAL

BASE CASE ANALYSIS	APPROX TOTAL CORE DAMAGE PROBAB.*		PROPOSED CORE MELT SAFETY GOAL	
	INTERNAL EVENTS	EXTERNAL EVENTS	INTERNAL EVENTS	EXTERNAL EVENTS
PWR	9E-5 - 1.5E-4	~1E-4 TO LESS THAN 1E-6 **	7E-5	3E-5
BWR w/ISO COND.	1E-4			
BWR w/ HPCI-RCIC	9E-5			
BWR w/ HPCS-RCIC	8E-6			

* SUM OF "MEAN" VALUES FOR ALL SEQUENCES
** DEPENDING ON PLANT SUSCEPTABILITIES

CONTAINMENT FAILURE INSIGHTS

CONTAINMENT TYPE	APPROX TIME TO CONT. FAILURE AFTER ONSET OF CORE DAMAGE*	MOST PROBABLE CONT. FAILURE MODE
ICE COND.	1 HR. AT OR AFTER AC RECOVERY	H2,STEAM SPIKE, OVERPRESSURE H2
SMALL DRY	2 HR. AFTER AC RECOVERY	H2,STEAM SPIKE,OVERPRESSURE H2
LARGE DRY	10 HR. AFTER AC RECOVERY	OVERPRESSURE H2
MARK I, MARK II	2-4 HR. 4-8 HR.	ELEC. PENETRATION FAILURE OVERPRESSURE
MARK III	10-15 HR. 1 HR TO AFTER AC RECOVERY	OVERPRESSURE H2

*FOLLOWING EARLY CORE DAMAGE SEQUENCES. SEQUENCES INVOLVING LATER FAILURES RESULT IN A LITTLE LONGER TIMES TO CONTAINMENT FAILURE

SUMMARY OF IMPORTANT RESULTS

- STANDBY RELIABILITY OF DHR SYSTEMS
- DC RELIABILITY & BATTERY CAPACITY INCLUDING INSTRUMENTATION & CONTROL
- COMMON SERVICE WATER DEPENDENCIES
- RX COOLANT PUMP SEAL LEAKAGE & STUCK-OPEN SRV
- CONTAINMENT SIZE & DESIGN PRESSURE
- OPERATOR TRAINING & PROCEDURES
- EXTERNAL EVENTS

SUMMARY OF IMPORTANT RESULTS BY MAJOR PLANT TYPE

PWR: INITIAL AFWS UNAVAIL.,BATTERY DEPLETION EFFECTS, & RCS INTEGRITY LOSS UNDER A PROLONGED BLACKOUT

BWR w/ISO COND: RCS INTEGRITY LOSS (STUCK-OPEN SRV OR RECIRC COOLANT PUMP SEAL LEAK)

BWR w/HPCI-RCIC: ABILITY TO OPERATE HPCI-RCIC UNDER A PROLONGED BLACKOUT

BWR w/HPCS-RCIC: INITIAL HPCS-RCIC UNAVAIL., & ABILITY TO OPERATE RCIC UNDER A PROLONGED BLACKOUT

HUMAN ACTIONS

- RECOVER OFFSITE OR ONSITE POWER
- EXTEND BATTERY LIFE
- UPON RESTORATION OF AC, HAVE PLAN FOR WHICH SYSTEMS WILL BE PLACED BACK IN TO SERVICE & IN WHAT ORDER

CONCLUSIONS

HOW IMPORTANT IS STATION BLACKOUT?

NO ONE ANSWER EXISTS

DEPENDS ON PLANT FEATURES/OPERATION

ANALYSES & SENSITIVITIES:

- COVER VARIETY OF PLANT DESIGNS
- PROVIDE INFO FOR REVIEW OF SPECIFIC PLANTS

RELIABILITY OF EMERGENCY AC POWER SUPPLIES AT NUCLEAR POWER PLANTS

R.E. Battle

Oak Ridge National Laboratory

D.J. Campbell

JBF Associates, Inc.

T7, T8

PURPOSE

o PROVIDE TECHNICAL BASIS TO BE USED FOR RESOLUTION OF TAP A-44, STATION BLACKOUT

ESTIMATE THE RELIABILITY OF AC POWER SYSTEMS

IDENTIFY FACTORS IMPORTANT TO RELIABILITY

ESTIMATE THE COSTS OF IMPROVING AC POWER SYSTEMS

SCOPE

- OFFSITE POWER
  - DESIGN REVIEW
  - DATA ANALYSIS

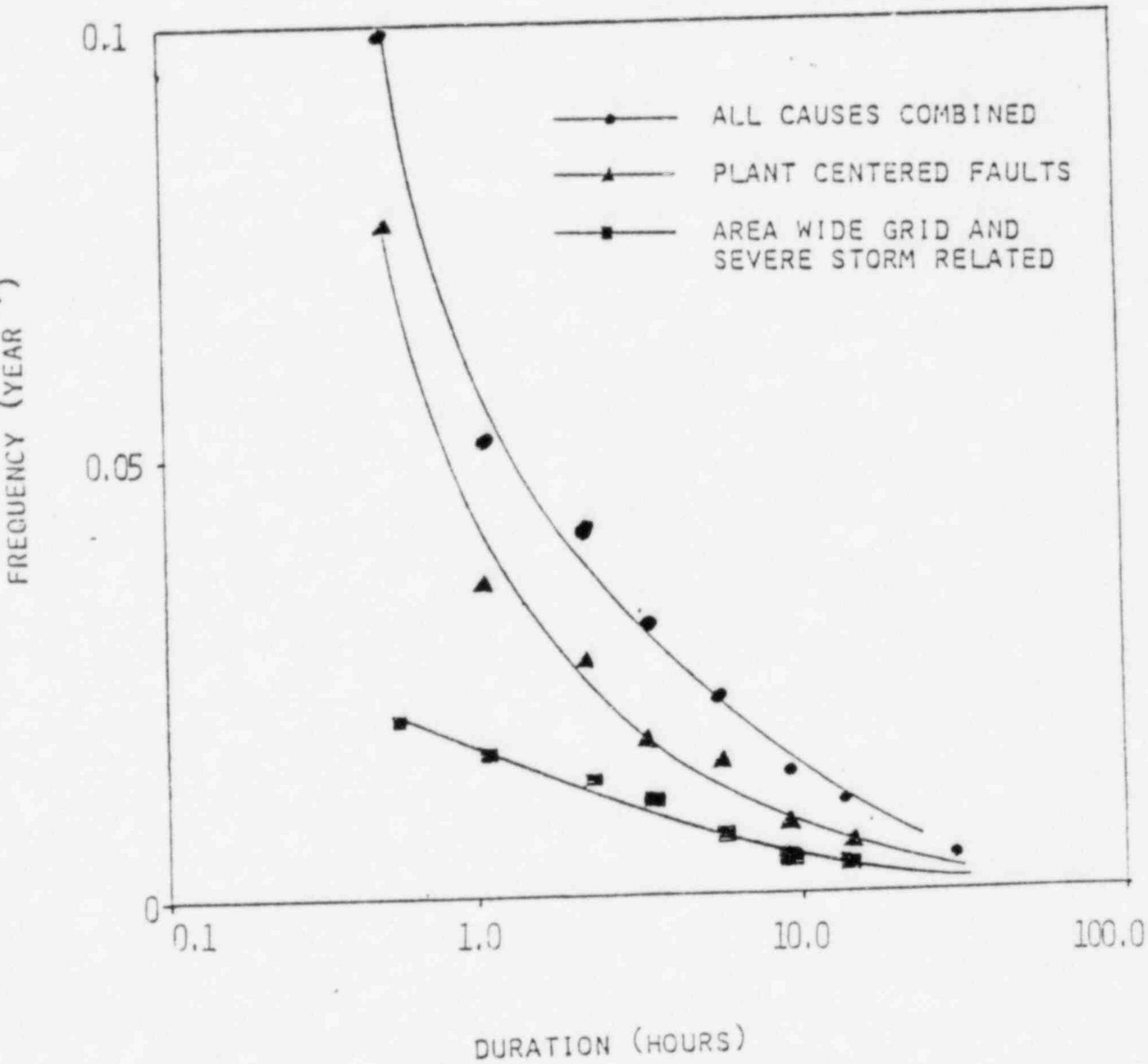
- ONSITE POWER
  - DESIGN REVIEW
  - OPERATIONS EXPERIENCE REVIEW
  - RELIABILITY ANALYSIS

LOSS OF OFFSITE POWER

FREQUENCY AND RESTORATION BY CAUSE

IMPORTANT DESIGN AND OPERATIONAL FACTORS

GENERIC FREQUENCY AND DURATION RELATION FOR LOSS OF ALL OFFSITE POWER



FACTORS AFFECTING OFFSITE POWER AVAILABILITY

- DESIGN
  - SWITCHYARD INTERCONNECTIONS
  - ALTERNATE POWER SOURCES

- OPERATION
  - RESTORATION PROCEDURES FOR PLANT AND SYSTEM DISPATCHER

    RESTORATION PROBABILITY IS BEING ANALYZED FURTHER

- GEOGRAPHICAL
  - GRID STABILITY AND SECURITY
  - WEATHER

    THE PROBABILITY OF FAILURE BECAUSE OF SEVERE WEATHER IS BEING ANALYZED FURTHER

ONSITE AC POWER SYSTEM RELIABILITY

DESIGN REVIEW

OPERATING EXPERIENCE REVIEW

RELIABILITY ANALYSIS

BOUNDARIES AND LIMITS

- FSAR (PLUS) LEVEL OF DESIGN DETAIL AND PLANT SPECIFIC PROCEDURES
- USE INSIGHTS FROM AC RELIABILITY STUDIES IN OTHER PRAs AND PAST OPERATING EXPERIENCE
- LIMIT DEPTH OF ANALYSIS TO IDENTIFY POTENTIALLY IMPORTANT INTERACTIONS AND DEPENDENT FAILURES WHERE PLANT SPECIFIC DESIGN DETAILS VARY CONSIDERABLY
- ELECTRIC POWER REQUIREMENTS CONSIDERED FOR NORMAL SHUTDOWN AND SMALL LOCA WITH LOSS OF OFFSITE POWER
- SEPARATE ACCIDENT SEQUENCE STUDY

INTERACTIONS

- COOLING SUBSYSTEM
    - PLANT SERVICE-WATER-COOLED
    - AIR-COOLED
- DC CONTROL POWER
    - PLANT IE BATTERIES
    - DEDICATED BATTERIES
- OFFSITE POWER
    - CONTROL POWER
    - LOW VOLTAGE
    - PARALLEL SOURCES

DESIGN REVIEW OF EIGHTEEN PLANTS/UNITS

- SWITCHYARD
- DISTRIBUTION SYSTEM
- DC POWER SYSTEM
- DIESEL GENERATOR
  - ENGINE
  - GENERATOR
  - GOVERNOR
  - EXCITER AND REGULATOR
  - START SYSTEM
  - PROTECTION AND ALARM
  - COOLING SYSTEM
  - LUBE OIL SYSTEM
  - FUEL OIL SYSTEM
  - COMBUSTION AIR AND EXHAUST
- ELECTRICAL INTERFACES
- PROCEDURES

FOUR SITE VISITS

IDENTIFIED POTENTIAL CCF MODES

DIESEL GENERATOR CONFIGURATION

CONFIGURATION	NUMBER OF PLANTS/UNITS
1-OF-2	11
1-OF-3	1
2-OF-3	2
2-OF-4	2
2-OF-5	2

TWO DESIGNS WERE NOT MODELED

1-OF-1

3-OF-8

OPERATING EXPERIENCE

DATA SOURCES

STATISTICAL RESULTS

COMMON-CAUSE FAILURE

DATA SOURCES

STATION BLACKOUT QUESTIONNAIRE

36 PLANTS 90 DIESELS

FAILURES, DEMANDS, T&M UNAVAILABILITY, REPAIR TIME, AND MODIFICATIONS

NUREG-0737 QUESTIONNAIRE

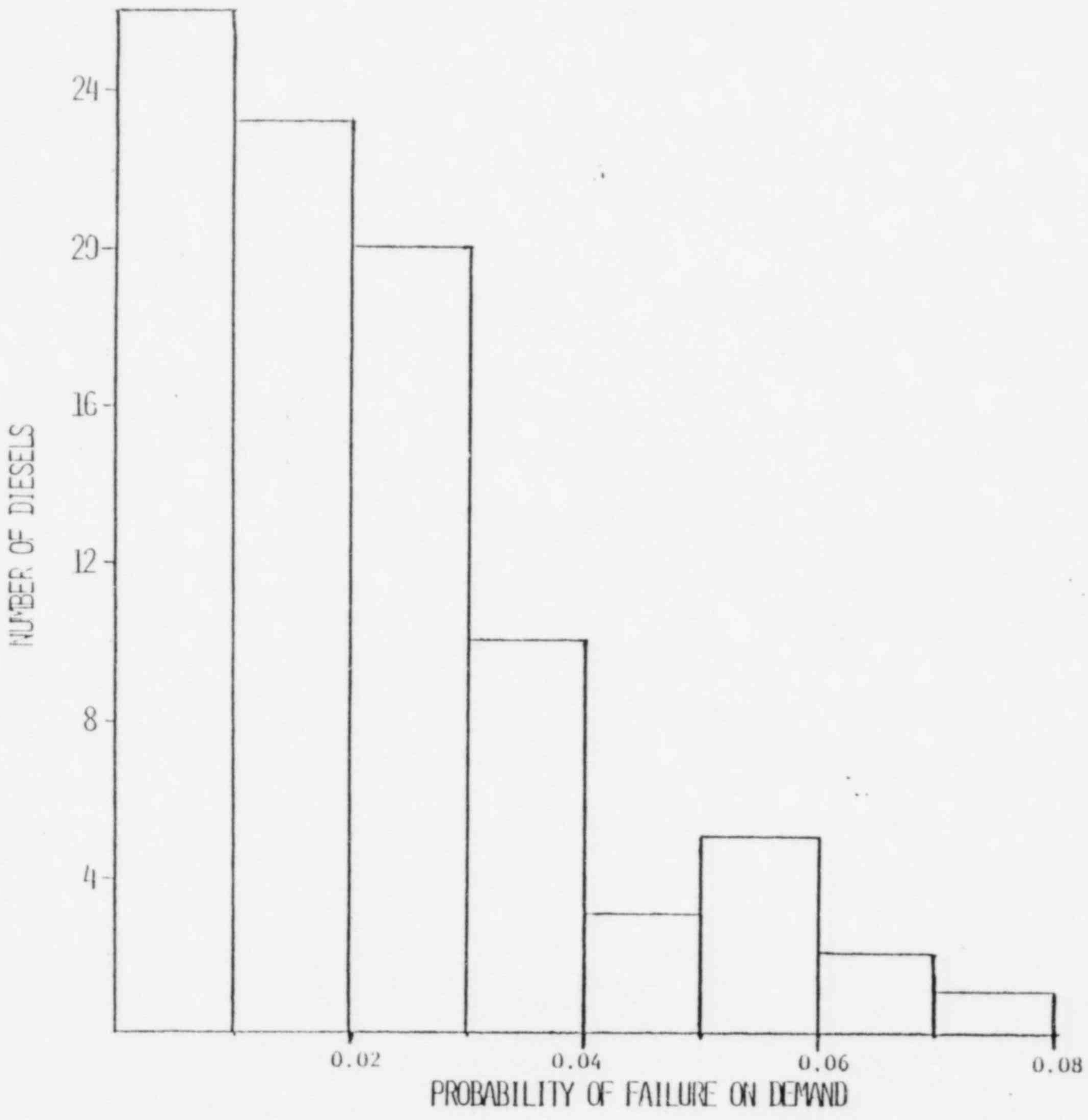
22 PLANTS 58 DIESELS

DIESEL OUTAGE AND DOWNTIME

LERs - 812 EVENTS

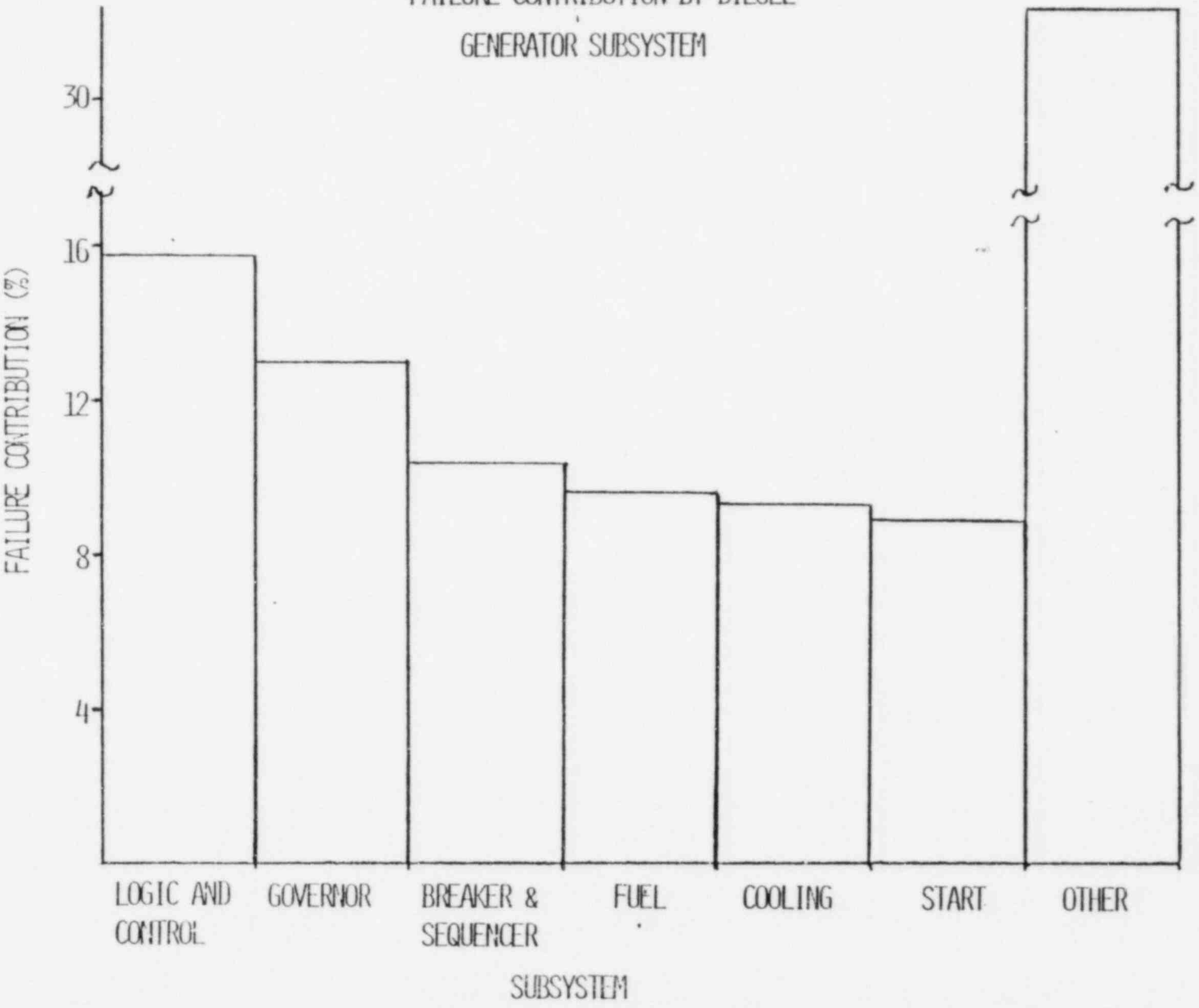
COMPARISON WITH EPRI STUDY

	ORNL			EPRI		
CATEGORY	AVERAGE	RANGE		AVERAGE	RANGE	
FAILURE/DEMAND	2×10^{-2}	2×10^{-3}	8×10^{-2}	2.3×10^{-2}	2.9×10^{-3}	8.8×10^{-2}
FAILURE TO RUN	2.4×10^{-3}	-	-	-	1.4×10^{-3}	1.5×10^{-2}
T&M UNAVAILABILITY INCLUDING REACTOR SHUTDOWN	1.4×10^{-2}	4×10^{-3}	9×10^{-2}	1.1×10^{-2}	7×10^{-3}	1.2×10^{-2}
MEAN TIME TO REPAIR (HOURS)	20	2.0	146	15	-	-
COMMON-CAUSE FAILURE	-	1×10^{-4}	4.2×10^{-3}	-	1.7×10^{-3}	8.4×10^{-3}
AVERAGE NUMBER OF DEMANDS PER YEAR	32	12	85	56	36	80


24
20
16
12
8
4
NUMBER OF DIESELS
0.02
0.04
0.06
0.08
PROBABILITY OF FAILURE ON DEMAND

T8

FAILURE CONTRIBUTION BY DIESEL GENERATOR SUBSYSTEM



HUMAN ERROR

COMMON-CAUSE FAILURE

CATEGORY	ACTUAL FAILURES	UNAVAILABLE	POTENTIAL
PROCEDURAL ERRORS CAUSED BY MAINTENANCE	1	7	51

- RANGE OF PROBABILITIES

  $7.2 \times 10^{-5} - 3.7 \times 10^{-3}$

- MAINTENANCE PROCEDURE QUALITY
  - CLARITY
  - DETAILED CHECKLISTS
  - TEST AND REVIEW AFTER MAINTENANCE
  - INDICATION OF NORMAL VALUES

HARDWARE COMMON-CAUSE FAILURE

CATEGORY	ACTUAL FAILURES	UNAVAILABLE	POTENTIAL
ENVIRONMENT, OPERATING CONDITIONS	2	0	10

° RANGE OF PROBABILITIES

$3.6 \times 10^{-5} - 1.8 \times 10^{-3}$

° DESIGN FEATURES WITH CCF POTENTIAL

- GENERIC
  FUEL BLOCKAGE
  EXTREME ROOM TEMPERATURE
- PLANT SPECIFIC
  SERVICE WATER BLOCKAGE
  WATER IN FUEL
  JACKET WATER CORROSION
  AIR-START INTERCONNECTIONS

T9

RELIABILITY ANALYSIS

FAULT TREE MODELS

HUMAN ERROR AND HARDWARE COMMON-CAUSE FAILURE RATES WERE CALCULATED USING BFR COMPUTER CODE

SERVICE WATER, DC, AND OFFSITE SYSTEMS FAILURE DATA WERE OBTAINED FROM OTHER SOURCES

DIESEL REPAIR MODEL

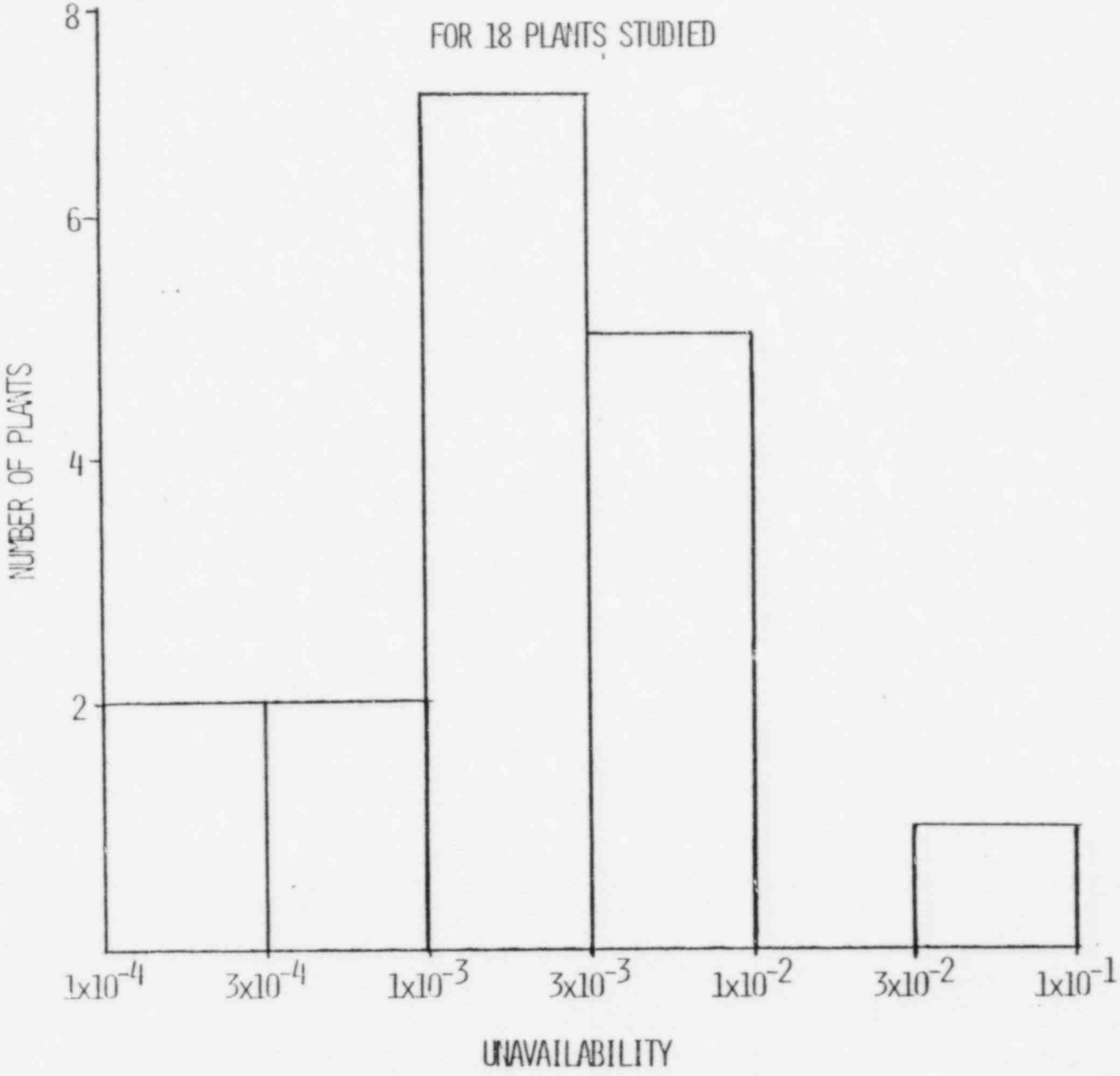
UNAVAILABILITY FOR T&M

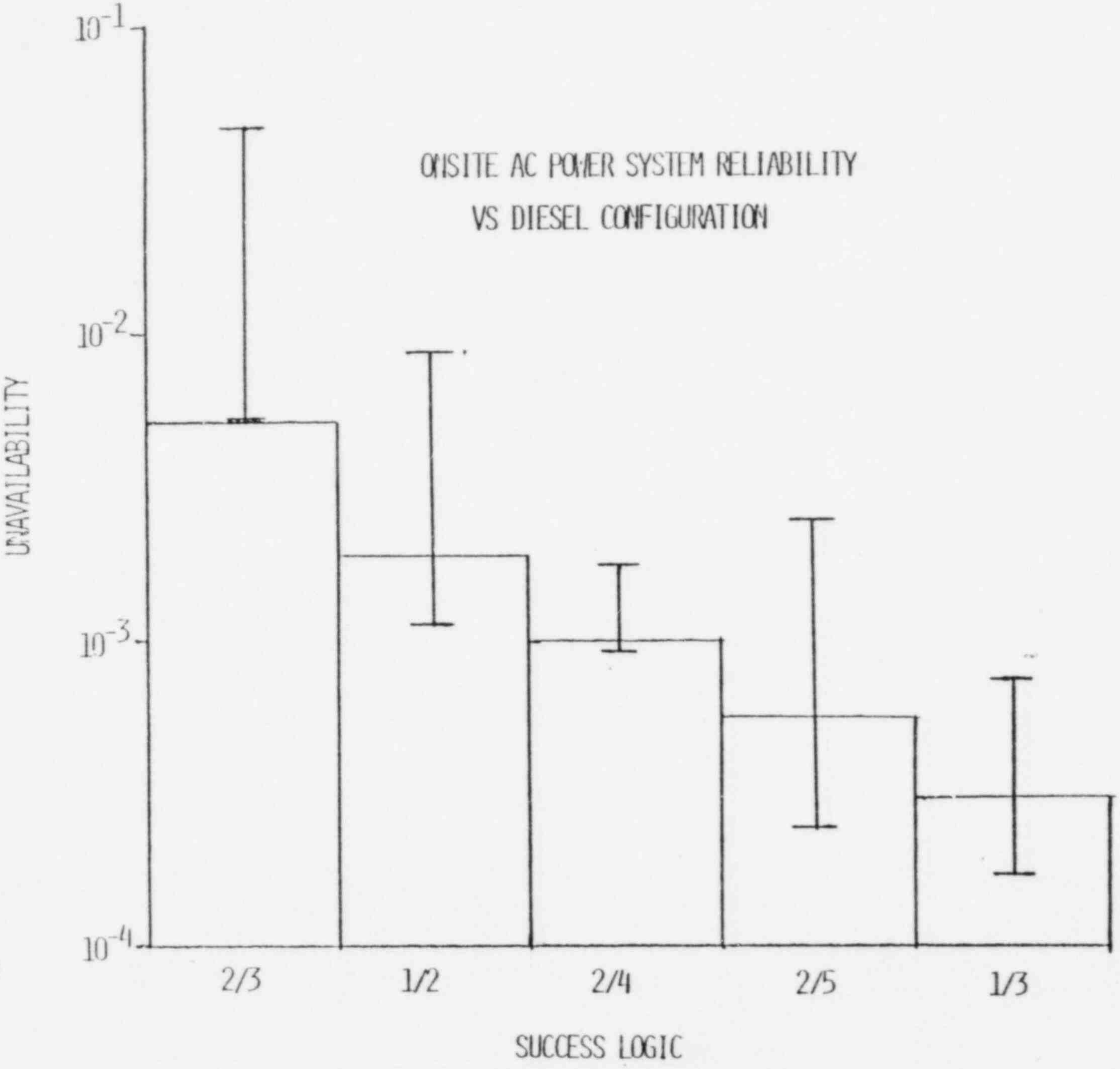
INDEPENDENT FAILURE

GENERIC AND PLANT SPECIFIC MODELS

ONSITE AC SYSTEM UNAVAILABILITY

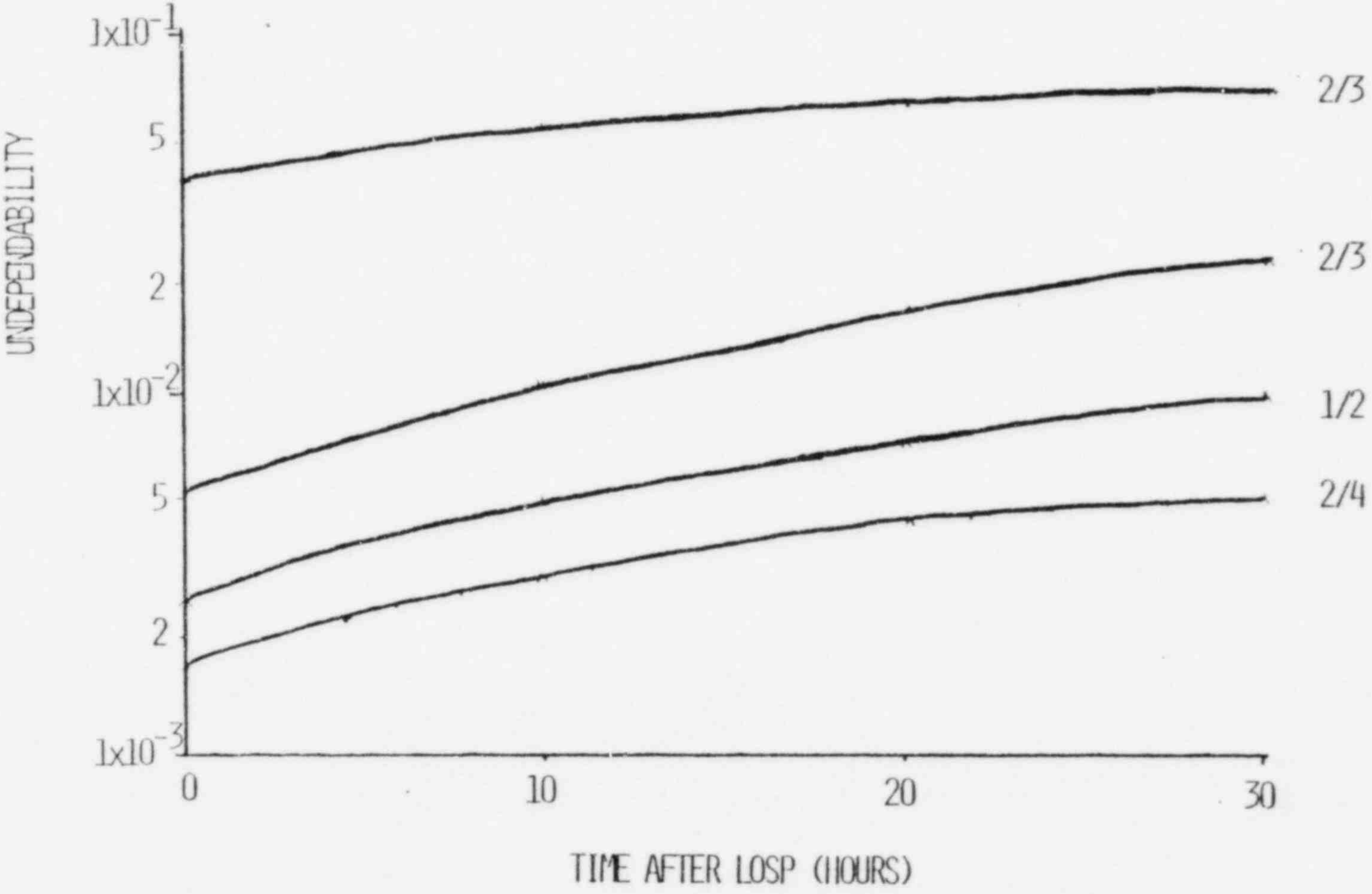
FOR 18 PLANTS STUDIED




ONSITE AC POWER SYSTEM RELIABILITY
VS DIESEL CONFIGURATION
UNAVAILABILITY
10^{-1}
10^{-2}
10^{-3}
10^{-4}
2/3
1/2
2/4
2/5
1/3
SUCCESS LOGIC

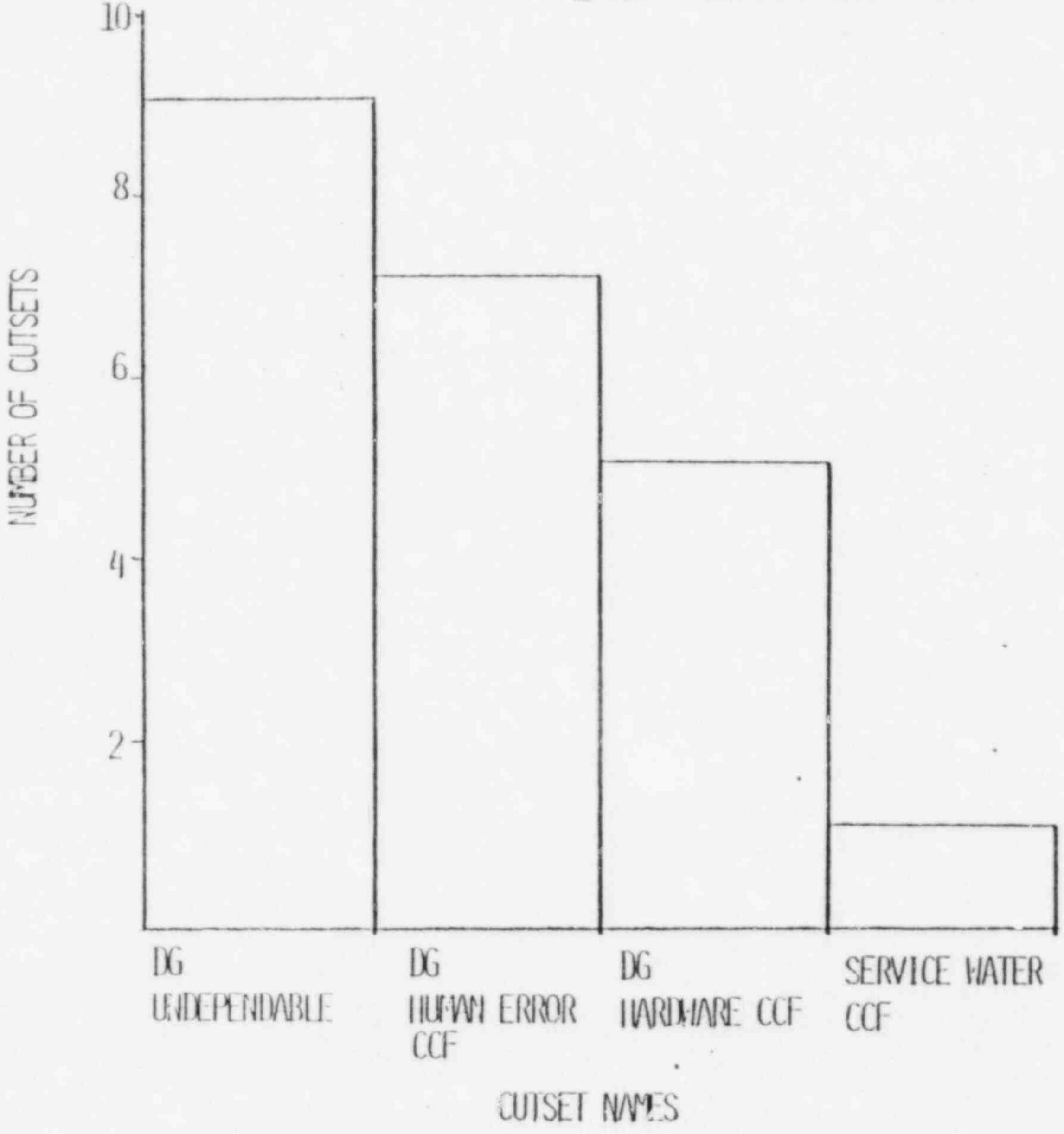
ONSITE AC SYSTEM UNDEPENDABILITY

VS TIME AFTER LOSP



CUTSETS WITH IMPORTANCE

≥ 0.20 FROM 18 PLANTS MODELED



6

SENSITIVITY

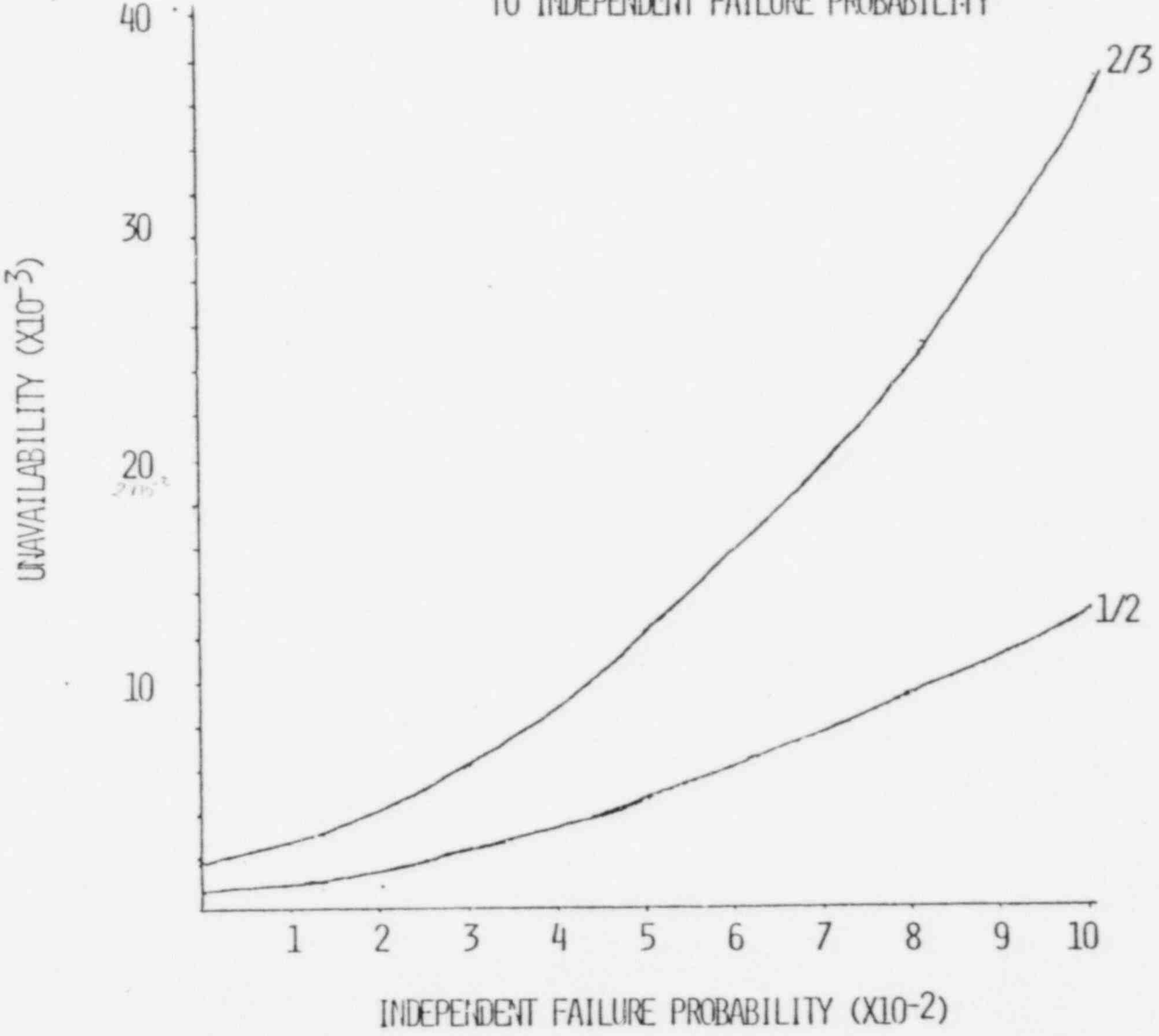
SENSITIVITY DEPENDS UPON:

- AC POWER SYSTEM CONFIGURATION
- DOMINANT FAILURE MODES AT THE PLANT

DIESEL CONFIGURATION AND BASIC EVENTS OF MOST IMPORTANCE

1-OF-2	DIESEL UNDEPENDABILITY DIESEL CCF
2-OF-3	DIESEL UNDEPENDABILITY DIESEL CCF DIESEL T&M
2-OF-4	DIESEL CCF DIESEL UNDEPENDABILITY SERVICE WATER UNDEPENDABILITY
1-OF-3	DIESEL CCF SERVICE WATER CCF
2-OF-5	DIESEL CCF DIESEL UNDEPENDABILITY

SENSITIVITY OF 1-OF-2 AND 2-OF-3 CONFIGURATIONS
TO INDEPENDENT FAILURE PROBABILITY



Results of Onsite Power System Reliability Analysis

Diesel Generator Configuration	Range of System Unavailability per Demand	Dominant Failure Causes
2-of-3	$4.2 \times 10^{-3} - 4.8 \times 10^{-2}$	Independent diesel failure. Human error CCF.
1-of-2	$1.1 \times 10^{-3} - 6.8 \times 10^{-3}$	Independent diesel failure. Human error CCF. T&M outages.
2-of-4	$3.7 \times 10^{-4} - 1.7 \times 10^{-3}$	Human error and hardware CCF.
1-of-3	$1.8 \times 10^{-4} - 7.2 \times 10^{-4}$	Human error, hardware, and service water CCF. Independent diesel failure. DC power CCF.
2-of-5	$1.4 \times 10^{-4} - 2.5 \times 10^{-3}$	Human error, hardware, service water, and dc power CCF.

Onsite System Sensitivity Analysis

Basic Event, Plant, and Success Logic	Basic Event Failure Probability Changed		Onsite System Unavailability Changed	
	From	To	From	To
Independent failure				
Plant A, 2-of-3	8.2×10^{-2}	4.1×10^{-2}	4.8×10^{-2}	3.1×10^{-2}
Plant B, 1-of-2	5.9×10^{-2}	3.0×10^{-2}	4.2×10^{-3}	2.1×10^{-3}
Hardware CCF				
Plant C, 2-of-5	1.8×10^{-3}	8.6×10^{-5}	2.5×10^{-3}	8.0×10^{-4}
Plant D, 1-of-3	6.0×10^{-4}	2.4×10^{-5}	7.2×10^{-4}	1.5×10^{-4}
Human error CCF				
Plant E, 1-of-2	8.8×10^{-4}	3.4×10^{-4}	1.5×10^{-3}	1.0×10^{-3}
T&M unavailability				
Plant F, 2-of-3	4.5×10^{-2}	0	4.8×10^{-2}	2.5×10^{-2}

COSTS OF POSSIBLE MODIFICATIONS TO IMPROVE RELIABILITY

° INDEPENDENT FAILURE	
- INSTALL AIR DRIERS AIR-START SUBSYSTEM	$100,000/DIESEL
- GASKET RELAY CABINET DOORS	$ 10,000/DIESEL
- OVERHAUL GOVERNOR	$ 6,000/DIESEL
° HUMAN ERROR CCF	
- REWRITE TEST AND MAINTENANCE PROCEDURES	$ 5,000/PROCEDURE
° DESIGN FEATURE CCF	
- REMOVE AIR-START SUBSYSTEM INTERCONNECTIONS	$ 5,000/CONNECTION
- INSTALL DRAIN ON FUEL DAY TANK	$ 10,000/DIESEL
- ADD CORROSION INHIBITOR TO JACKET WATER	$ 500/DIESEL
° ADD A 3000KW DIESEL GENERATOR	$20-30M

NOTE: INDIRECT COSTS SUCH AS REACTOR DOWNTIME COULD BE $500,000 PER DAY.

CONCLUSIONS

- RELIABILITY IMPROVEMENTS ARE PLANT-SPECIFIC AND MUST BE DETERMINED FROM PLANT DESIGN AND EXPERIENCE
- IMPROVING TEST AND MAINTENANCE PROCEDURES IS AN EFFICIENT MEANS OF INCREASING RELIABILITY AT SOME PLANTS
- DESIGN RELATED CCF CAN BE IDENTIFIED AND FIXED INEXPENSIVELY WHERE APPROPRIATE
- PLANTS WITH THE LESS RELIABLE DIESEL CONFIGURATION AND ABOVE AVERAGE INDEPENDENT FAILURE PROBABILITIES MAY SIGNIFICANTLY INCREASE RELIABILITY. SOME ROOT CAUSES OF INDEPENDENT FAILURE ARE:
    - MOISTURE IN THE AIR-START SYSTEM
    - SWITCH AND RELAY FAILURE FROM MOISTURE, DIRT, AND VIBRATION
    - GOVERNOR OIL CONTAMINATION
- DEPENDENCE ON OTHER PLANT SYSTEMS MAY BE IMPORTANT IF THESE SYSTEMS ARE UNRELIABLE
- EXCESSIVE SCHEDULED MAINTENANCE DURING REACTOR OPERATION CAN BE A LARGE CONTRIBUTOR FOR THE LESS RELIABLE CONFIGURATIONS

BRIEFING FOR
ACRS SUBCOMMITTEE
ON
AC/DC POWER SYSTEMS

RECENT OPERATING EXPERIENCE WITH EMERGENCY DIESEL GENERATORS

J.T. Beard
ORAB/NRR
September 8, 1982

T03

AGENDA

- Sources of Information
- "Significant" Operating Events
- Emergency Technical Specifications Changes
- Types of Failures
- Comments - Event Reporting/Reliability Assessment
  - Shared Systems
  - Testing
  - General

SOURCES OF INFORMATION
ON OPERATING EXPERIENCE

I. DAILY REVIEW OF OPERATING "OCCURRENCES"

(NRR OPERATING EVENTS BRIEFINGS)

FOR PERIOD 4/81 THRU 7/82:

- 2000 "OCCURRENCES" DISCUSSED (6/DAY)
- 200 SIGNIFICANT OCCURRENCES (NRR BRIEFING)
- 8 INVOLVED EDG PROBLEMS (ONLY 3-4%)

II. REVIEW OF EMERGENCY TECH. SPECS CHANGES

- FARLEY STATION
  - 3 EMERGENCY T.S. CHANGES
  - 1 MAJOR T.S. CHANGE (FEB. 82)
- PEACH BOTTOM UNIT 2
- HATCH STATION
  - 2 EMERGENCY T.S. CHANGES
- BRUNSWICK STATION
- PALISADES - JANUARY 1981

  DISCONNECTION OF BOTH DC BATTERIES FOR ONE HOUR.

  - AUTOMATIC START AND LOADING OF EDG'S WOULD NOT HAVE OCCURRED ON LOW OF OFFSITE POWER.

SIGNIFICANT EDG EVENTS

- Millstone 2 --- January 1981

  Human error caused loss of one of two redundant D.C. power systems, which led to loss of one of two offsite A.C. circuits and auto-start for both EDG's. Subsequently, one EDG tripped due to mechanical failure; other EDG tripped when D.C. power was restored, due to design.

- Millstone 1 --- April 1981

  Single failure of breaker-position relay could have prevented both EDG's from tying into 4kv buses.

- Hatch 1 --- April 1981

  Failure of two undervoltage relays (associated with startup transformer) during testing prevented 2 EDG's from tying into 4kv buses.

- Dresden 2/3 --- October 1981

  Shared EDG and Unit 3 EDG tripped during routine test due to lack of water cooling (air binding).

- Dresden 2/3 --- November 1981

  Unit 3 EDG failed--repeat of October occurrence. Defective check valves in cooling water line. All 3 EDG's at station effected.

SIGNIFICANT EDG EVENTS (CONTINUED)

- CALVERT CLIFFS 1/2 --- JUNE 1981

  TEMPORARY LOSS OF ALL 3 EDG'S AND PARTIAL LOSS OF OFFSITE POWER.

  - UNIT 1 EDG OUT-OF-SERVICE, ROUTINE MAINTENANCE.
  - ONE OFFSITE CIRCUIT TAKEN OUT-OF-SERVICE - PAINTING.
  - SHARED EDG TRIPPED - CHRONIC VOLTAGE REGULATOR PROBLEM.
  - UNIT 2 EDG TRIPPED - OPERATOR ERROR.

- QUAD CITIES 1/2 --- JUNE 1982

  TEMPORARY LOSS OF 2 OF 3 EDG'S FOR STATION AND ALL OFFSITE POWER TO UNIT 2.

  - UNIT 1 EDG OUT-OF-SERVICE, ROUTINE MAINTENANCE.
  - UNIT 2 STARTUP TRANSFORMER TAKEN OUT-OF-SERVICE FOR ROUTINE MAINTENANCE.
  - UNIT 2 TRIPPED - LOSS OF ALL OFFSITE TO UNIT.
  - SHARED EDG STARTED, TRIPPED - IMPROPER ADJUSTMENT.
  - UNIT 2 EDG STARTED, RAN OKAY.

- SAN ONOFRE 1 --- JULY 1982

  LUBE OIL FIRE DURING ROUTINE TEST, ONLY 1 EDG AFFECTED.

EMERGENCY TECHNICAL SPECIFICATION CHANGES

- FARLEY STATION - MAY 1981
  - MAJOR FAILURE OF EDG 1C - FAIRBANKS-MORSE 2850 KW.
  - EDG 1C SHARED - DIV. A, EITHER UNIT.
  - JACKET COOLING WATER FOUND IN HEADS OF 2 CYLINDERS.
  - O-RING SEAL PROBLEM.
  - REPAIR, TEST TIME REQUIRED - 13 DAYS.
  - 10-DAY LCO ACTION STATEMENT EXT. GRANTED - BOTH UNITS.
  - ACTION STATEMENT TESTING CHANGED FROM EVERY 8 HOURS TO EVERY 72 HOURS.

- FARLEY STATION - JULY 1981
  - MAJOR FAILURE OF EDG 1C - FAIRBANKS-MORSE 2850 KW.
  - JACKET WATER FOUND IN HEADS OF 4 CYLINDERS.
  - WORN WRIST PINS, BUSHINGS CAUSED O-RING FAILURES.
  - EDG 1C HAD BEEN TEST STARTED EVERY 3 DAYS - RG 1.108.
  - REPAIR TIME 15 DAYS.
  - 12-DAY EXTENSION GRANTED.
  - ACTION STATEMENT TESTING RELAXED TO EVERY 72 HOURS.

- FARLEY STATION - SEPTEMBER 1981
  - MAJOR FAILURE OF EDG 2C - FAIRBANKS-MORSE 2850 KW.
  - EDG 2C SHARED - DIV. B, EITHER UNIT.
  - WATER IN ONE CYLINDER HEAD, THRUST BEARINGS AND CRANKSHAFT BEARINGS WIPED.

EMERGENCY TECHNICAL SPECIFICATION CHANGES (CONTINUED)

- FARLEY STATION - SEPTEMBER 1981 (CONTINUED)
  - REPAIR TIME NEEDED - 17 DAYS.
  - 14-DAY EXTENSION GRANTED.
  - ACTION STATEMENT TESTING RELAXED TO EVERY 72 HOURS.
  - PERMANENT T.S. CHANGES REQUESTED BY NRC.
- PEACH BOTTOM UNIT 2 - SEPTEMBER 1981
  - EDG "D" FAILED - FAIRBANKS-MORSE 2600 KW.
  - REPAIR TIME NEEDED - 10 DAYS.
  - 3-DAY LCO EXTENSION GRANTED.
  - ACTION STATEMENT TESTING - TWICE PER DAY.
- HATCH UNIT 2 - DECEMBER 1981
  - MAJOR FAILURE OF EDG 2C - FAIRBANKS-MORSE 2850 KW.
  - EDG 2C IS DEDICATED TO 1 OF 2-OUT-OF-3 BUSES FOR UNIT 2.
  - THREW A ROD ON ONE CYLINDER - REPEAT OF DEC. 1980 FAILURE.
  - REPAIR TIME REQUIRED - 18 DAYS.
  - EDG 2A FAILED DURING 3-DAY LCO - REPAIRED IN 6 HOURS.
  - 15-DAY LCO EXTENSION GRANTED.
  - ACTION STATEMENT TESTING RELAXED TO EVERY 72 HOURS.
- BRUNSWICK STATION - JULY 1982
  - MAJOR FAILURE OF EDG 2 - NORDBERG 3500 KW.
  - EDG IS DEDICATED TO 1 OF 3-OUT-OF-4 BUSES FOR STATION - NON-UNITIZED DISTRIBUTION SYSTEM.
  - SUPPORT SYSTEM DRIVE BROKEN LOOSE.

EMERGENCY TECHNICAL SPECIFICATION CHANGES (CONTINUED)

- BRUNSWICK STATION - JULY 1982 (CONTINUED)
  - REPAIR TIME REQUIRED - 7 DAYS.
  - 4-DAY LCO EXTENSION GRANTED.
  - NRC CONCERNS REGARDING OTHER EDG'S AT STATION.
  - METALLURGICAL REPORT - FATIGUE DUE TO EXCESSIVE STARTS (1638).
  - OTHER EDG'S INSPECTED PRIOR TO PLANT S/U - 3 OF 4 EDG'S SAME PROBLEM.
- HATCH STATION JULY 1982
  - MAJOR FAILURE OF EDG 2C - FAIRBANKS-MORSE 2850 KW.
  - CONNECTING ROD "FAILED."
  - REPAIR TIME REQUIRED - 18 DAYS.
  - FOLLOWING NRC REVIEW, REQUEST FOR EMER. T.S. CHANGE WITHDRAWN.
  - PLANT SHUTDOWN FOR EDG REPAIRS.
  - DURING POST-MAINT. TESTING - EDG 2C FAILED AGAIN - MAIN AND ROD BEARINGS WIPED.
  - OTHER EDG'S INSPECTED - 3 OF 4 SAME PROBLEM.

TYPES OF FAILURES

- 1959-1973 EXPERIENCE (PUBLISHED 1975):
  - MAJOR PROBLEM IS STARTING 35%.
  - OTHER PROBLEMS: ENGINE, GOVERNOR, COOLING 19-12% EACH.

    NOTE: REG. GUIDE 1.108 ISSUED 1977.
- 1976-1978 EXPERIENCE:
  - STARTING NO LONGER THE MAJOR PROBLEM.
  - GOVERNOR, STARTING, FUEL OIL PROBLEMS 17-12% EACH.
- APPARENT PROBLEM AREAS (1976-1978 EXPERIENCE):

  FAIRBANKS-MORSE 2850 KW (16% POPULATION):
  - MORE FAILURES/MACHINE (24% OF ALL FAILURES).
  - HIGHER PERCENTAGE OF LONG REPAIR TIMES (>24 HOURS) 16% OF FAILURES (COMPARED TO AVERAGE OF 10%).
- NUMBER OF TEST STARTS
  - SOME EDG'S GETTING 16-18 STARTS/MONTH.
  - REG. GUIDE 1.108 3-DAY TESTING.
  - ACTION STATEMENT 8-HOUR TESTING.

COMMENTS

(•• MAJOR COMMENTS)

RECENT OPERATING EXPERIENCE SEEMS TO INDICATE:

I. EVENT REPORTING/RELIABILITY ASSESSMENTS

- RELIABILITY ASSESSMENTS SHOULD BE BASED ONLY UPON TECHNICAL ANALYSIS OF THOSE OCCURRENCES IN WHICH AN EDG WOULD HAVE BEEN INCAPACITATED DURING A NEED FOR EMERGENCY POWER.
- •• EVEN THOUGH AVERAGE EDG RELIABILITY MAY BE SATISFACTORY THE EXTREMES ARE SIGNIFICANT AND WARRANT ATTENTION.

II. DESIGNS WITH SHARED EQUIPMENT

- MOST INTERESTING EVENTS HAVE INVOLVED MULTI-PLANT STATIONS, OFTEN WITH SHARED EQUIPMENT.
- •• STATIONS DESIGNED FOR ONLY A SINGLE FAILURE PER STATION RATHER THAN FOR A SINGLE FAILURE PER PLANT (UNIT) ARE MORE VULNERABLE TO MAJOR EVENTS.
- •• WHEN A SHARED EDG HAS A PROBLEM, BOTH PLANTS LCO'S COME INTO PLAN AND BOTH PLANTS MAY HAVE TO COME DOWN.
- •• IN SOME CASES, THE ASSIGNMENT OF SUPPORT SYSTEMS (E.G., RHR SERVICE WATER) TO THE EMERGENCY POWER BUSES MAY BE CRUCIAL AND LIMITING. FOR EXAMPLE: 2 UNIT STATION MAY REQUIRE 4 OUT OF 5 EDG'S FOR SIMPLY A LOSS-OF-OFFSITE-POWER, WITHOUT A REACTOR TRANSIENT OR ACCIDENT.
- IN SOME CASES, THE ONSITE DISTRIBUTION SYSTEM DESIGN IS BASED UPON PROVIDING POWER TO THE STATION AS A WHOLE RATHER THAN ON A PER PLANT BASIS. LOSS OF ANY EDG IMPACTS BOTH PLANTS AND COMPLICATES SAFETY CONSIDERATIONS.

COMMENTS (CONTINUED)

III. Testing Requirements

•• Requirement for routine test-starts every 3 days has contributed to failures and should be reconsidered. 14-day and 7-day test intervals appear to be optional.

•• Testing should be focused upon identifying "unreliable EDG's." Major corrective action should follow, not just more testing.

•• Testing frequency during LCO Action Statements should be relaxed to: 4-8 hours (vs. 1 hour) for initial test to rule out common causes. 48-72 hours (vs. 8 hours) for repeat test starts.

• Manufacturer's recommendations should be re-evaluated to determine if adequate internal engine inspections are required after X starts and Y hours of operation.

IV. General

• Licensees should be careful regarding taking an offsite circuit out-of-service for routine reasons when any EDG is already out-of-service and vice-versa.

• When major failures occur, neither a 3-day nor a 7-day LCO will cover repair time. Hence, requests for emer. T.S. changes.

Goal: Improve the capability to deliver standby power using diesel generator (DG) systems.

Method: Modify startup requirements

Capability =

f(reliability, operating procedures)

Estimated Reliability of DG Systems

DG system actuated during:	Estimated reliability (%)	95-Percent confidence interval
testing	98.1	97.9 – 98.3
loss of offsite power	97.4	92.9 – 99.2
other safety injections	97.4	96.1 – 98.7
any startup	98.1	97.9 - 98.3

The number of attempted and successful startups was presented by Baranowsky at the 30 March 1982 meeting of the ACRS Subcommittee on AC/DC Power Supply Reliability.

Engine Wear

During a rapid startup, engine wear is caused by:

Large dynamic forces,

Insufficient oil to lubricate components,

Insufficient air to burn fuel -

- fuel explodes
- lubicating oil burns

Heterogeneous component heating.

Improve DG System Capability

Modify equipment (DG systems already installed)

- circulate lubricating oil under pressure
- other

Change maintenance procedures

Require several small engines instead of one large engine to drive a single generator (DG systems yet to be installed)

- SONGS, Units 2 and 3

Change operating procedures.

Change Operating Procedures to Reflect Engine Characteristics

Engine characteristics:

- an inherent level of unreliability.
- engine wear during rapid startups.

Recognize:

- a well defined purpose for testing
  - verify that a DG system operates
  - verify that a DG system rapidly starts.
- standby power is rarely needed immediately on demand.

Slow Starting a DG System

-Testing

Frequent slow startups verify that a DG system operates.

Occassional rapid startups verify that a DG system rapidly starts.

Slow Starting a DG System
- On Demand

During a loss of offsite power, a reactor can be maintained in a safe condition without standby power.

- Inspect.
- Slow start.

Some demands can be anticipated

... grid problems may lead to a collapse of (a portion of) the electrical grid

... storms may open breakers or tear power lines.

... switch yard activities may inadvertently open breakers.

- Inspect.
- Slow start a DG system whenever a loss of offsite power is likely.

Recommendations

Modify DG system startup requirements, both during testing and on demand, to include slow startups

The End

DRAFT BTP PSB-3
GUIDELINES FOR ENHANCING RELIABILITY OF DC POWER SYSTEMS

RECOMMENDATION #1 OF NUREG-0666

PROHIBIT DESIGN AND OPERATIONAL FEATURES WHICH COULD COMPROMISE DIVISION INDEPENDENCE

PSB POSITION 1

- ELECTRICAL INTERCONNECTIONS BETWEEN REDUNDANT DIVISIONS:

  (1) ACCOMPLISHED BY MANUAL MEANS ONLY

  (2) RESTRICT USE ONLY DURING COLD SHUTDOWN

  (3) STRICT ADMINISTRATIVE CONTROL

  (4) SINGLE FAILURE DESIGN

    (A) TWO SERIES DISCONNECT DEVICES

    (B) ALARM UPON CLOSURE

  (5) RESTRICT USE BETWEEN DC SYSTEMS AT MULTIUNIT STATIONS

T19

MULTI PLANT ACTION ITEM
(NOT PART OF NUREG-0666 STUDY)

AVAILABILITY OF ANNUNCIATORS AND MONITORING SYSTEMS TO THE CONTROL ROOM OPERATOR

PSB POSITION 2

- ALARMS (CONTROL ROOM)
  - (1) BATTERY CIRCUIT OPEN
  - (2) BATTERY CHARGER CIRCUIT OPEN
  - (3) GROUND FAULT
  - (4) BUS UNDERVOLTAGE
  - (5) BUS OVERVOLTAGE
  - (6) CHARGER FAILURE
  - (7) BATTERY DISCHARGE
- MONITORS (LOCAL OR CONTROL ROOM)
  - (1) BUS VOLTAGE
  - (2) BATTERY INPUT CURRENT
  - (3) BATTERY OUTPUT CURRENT
  - (4) CHARGER OUTPUT CURRENT
- FAILURE OF ONE BATTERY BUS SHALL NOT CAUSE TOTAL LOSS OF THE CONTROL ROOM ANNUNCIATOR SYSTEM

MULTI PLANT ACTION ITEM
(NOT PART OF NUREG-0666 STUDY)

DC SYSTEM BYPASS STATUS INDICATION

PSB POSITION 3

- BYPASS AND INOPERABLE STATUS INDICATION
  1. (1) BATTERY OUTPUT BREAKER
  2. (2) CHARGER INPUT AND OUTPUT BREAKER

RECOMMENDATION 2 OF NUREG-0666

REDUCE THE LIKELIHOOD OF BATTERY DAMAGE

RECOMMENDATION 3 OF NUREG-0666

MINIMIZE THE POTENTIAL FOR HUMAN ERROR-RELATED COMMON CAUSE FAILURE

PSB POSITION 4

- WRITTEN PROCEDURES AND ADMINISTRATIVE CONTROLS
  - (1) PREVENT ACTIVITIES ON REDUNDANT DIVISIONS AT THE SAME TIME
  - (2) REVIEW ACTIVITIES TO MINIMIZE HUMAN ERROR CAUSING MORE THAN ONE DIVISION TO BE UNAVAILABLE
  - (3) ASSURANCE THAT ACTIVITIES ARE DONE CORRECTLY:
    - (A) ROTATION OF PERSONNEL
    - (B) VERIFICATION OF COMPLETED WORK

RECOMMENDATION 2 OF NUREG-0666

- PREVENTIVE MAINTENANCE ON BUS CONNECTIONS
- DC POWER AVAILABILITY FROM THE BATTERY TO THE BUS

PSB POSITION 5

- TECHNICAL SPECIFICATION REQUIREMENTS CURRENTLY IMPOSED ON NTOL'S

  (1) VISUAL INSPECTION AND MEASURED RESISTANCE OF BUS AND BATTERY TERMINAL CONNECTIONS

  (2) BATTERY SERVICE TEST

RECOMMENDATION 4 OF NUREG-0666

MAINTAIN REACTOR CORE COOLING GIVEN
- THE LOSS OF ANY DC BUS AND
- A SINGLE INDEPENDENT FAILURE

PSB POSITION 6A

- GIVEN A FAILURE OF ONE DC BUS:
  - (1) REDUNDANT CAPABILITY FOR REACTOR COOLING
  - (2) REACTOR COOLANT SYSTEM INTEGRITY AND ISOLATION CAPABILITY
  - (3) ADEQUATE OPERATING PROCEDURES, INSTRUMENTATION, AND CONTROL FUNCTIONS
- CONSIDERATION AND ASSUMPTIONS:
  - (1) DURATION
  - (2) TRANSIENT CONDITIONS AND INTERACTIONS
  - (3) SYSTEM AND COMPONENTS ASSOCIATED WITH FAILED BUS
    - (A) UNAVAILABLE FOR SHUTDOWN COOLING
    - (B) NOT CONSIDERED SINGLE INDEPENDENT FAILURE
  - (4) FAILURE OF REDUNDANT DC SYSTEM NEED NOT BE CONSIDERED
  - (5) SHUTDOWN SYSTEMS AND COMPONENTS
    - (A) SAFETY GRADE, OR
    - (B) USED REGULARLY, OR
    - (C) SUBJECT TO ROUTINE OPERABILITY CHECKS
  - (6) SINGLE FAILURE MEANS SINGLE ACTIVE FAILURE

ALTERNATIVE
TO RECOMMENDATION 4 OF NUREG-0666

IMPROVE THE AVAILABILITY OF REACTOR SHUTDOWN COOLING SYSTEMS

POSITION 6B

NON-SAFETY DC SYSTEMS

- PROVIDES POWER FOR:
  1. NORMAL (NON-ACCIDENT) SHUTDOWN COOLING LOADS
  2. OFFSITE AC POWER CIRCUIT CONTROL, PROTECTION AND SURVEILLANCE LOADS
  3. ALL NON-SAFETY LOADS EXCEPT FOR CRITICAL LOADS
- INDEPENDENCE
- MONITORING
- SIZING

POSITION 7

SIZING OF SAFETY DC SYSTEM

POSITION 8

NUMBER OF SAFETY DC SYSTEM DIVISIONS

MATRIX OF OPTIONS FOR APPLYING BTP-PSB-3

<table>
<tr><th>REVIEW STAGE
OPTIONS</th><th>OR</th><th>OL</th><th>CP</th></tr>
<tr><td>1</td><td>POSITIONS 1 TO 5</td><td>----</td><td>----</td></tr>
<tr><td>2</td><td colspan="2">POSITIONS 1 TO 5 AND 6A</td><td>----</td></tr>
<tr><td>3</td><td>----</td><td colspan="2">POSITIONS 1 TO 5, 6B AND 7</td></tr>
<tr><td>4</td><td>----</td><td colspan="2">POSITIONS 1 TO 8</td></tr>
</table>

NOTE:
POS. 1 - INTERCONNECTION
POS. 2 & 3 - MONITORING
POS. 4 - PROCEDURES
POS. 5 - TECHNICAL SPECIFICATIONS
POS. 6A - MULTIPLE FAILURE ANALYSIS
POS. 6B - BOP & SWITCHYARD BATTERIES
POS. 7 - BATTERY SIZING
POS. 8 - FOUR DIVISIONS OF CLASS 1E BATTERIES