AR

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS,

SUBCOMMITTEE ON AC/DC POWER SYSTEMS RELIABILITY.

Room 1046,
1717 H Street Northwest,
Washington, D.C.

Thursday, January 22, 1981.

The subcommittee met at 8:32 a.m., chaired by Jeremiah Ray.

ACRS Members Present:

JEREMIAH RAY, Chairman
J. EBERSOLE
W. MATHIS
W. KERR

ACRS Consultants Present:

E. EPLER
W. LIPINSKI
P. DAVIS

8101260442

THIS DOCUMENT CONTAINS POOR QUALITY PAGES

NRC Staff Present:

F. ROSA
J. BICKEL
R. FITZPATRICK
D. BASDEKAS
R. EDISON
P. BARANOWSKY
J. FEDELE
A. KOLACZKOWSKI

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

arl

PROCEEDINGS

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

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

I am Jerry J. Ray, Subcommittee chairman. The other ACRS members present today are Mr. Ebersole, immediately on my left; and then in order, Mr. Mathis.

And the ACRS consultants present so far are Mr. Epler and Dr. Lipinski, in the order left to right from where I sit.

Mr. Davis, the third consultant, will be here later, and the fourth member of the subcommittee, Dr. Kerr, is expected later today.

The purpose of this meeting is to review a number of issues related to the reliability of the AC/DC power systems used in nuclear power plants.

This is the first meeting of this subcommittee. The specific charge which has been given to this subcommittee is to review the reliability of existing systems and formulate recommendations as to reliability goals and improvements which might be made to these systems.

To achieve this goal, it is my intention to hold subcommittee meetings in the future, during which I would solicit additional input from the NRC Research and Licensing

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

ar4

Staff, and from members of industry and the public, and I would emphasize the last point, members of the industry and the public.

This meeting is being conducted in accordance with the p. .ions of the Federal Advisory Committee Act and the Government in the Sunshine Act.

Richard Savio, immediately on my right, is a designated federal employee for the meeting.

The rules for participation at today's meeting have been announced as part of the notice of this meeting previously published in the Federal Register on January 6th, 1981.

A transcript of the meeting is being kept and will be made available within five working days. It is requested that each speaker first identify himself and speak with sufficient clarity and volume so that he can be readily heard, and to this extent, if you do not have a speaker at your place, I would request that you move forward to the one of the speakers that is available at the counsel tables.

We have received no written comments or requests for time to make oral statements from members of the public, but I would add that should anyone feel he would like to make comments, we would like to be advised as soon as possible, so that we can allow time for such.

We will proceed with the meeting, and I call upon -- we will immediately have an executive session for a period, and we expect the first NRC presenter to be Robert Fitzpatrick of the NRC Staff.

I would like to add that Mr. David Bessette with the ACRS Technical Staff is participating in the meeting, and he is sitting here to my right, next to Dr. Savio.

To the members of our subcommittee and the consultants, I have previously issued and this morning there has been placed at your positions, Mr. Epler and Dr. Lipinski, a memorandum which I prepared on August 8, outlining the questions which at that time I conceived we might wish to address in the course of developing an outline for this subcommittee.

I was wondering if any of the subcommittee members have any comments on this as to what our goals should be, and what our subjects of activity would be, other than what might follow from today's activities.

My concerns at that time centered around the thought that perhaps our basic initial activities might very well be a review of what today's practices are on the part of the NRC Staff, and in that sense start with what are the present regulatory requirements.

I was wondering if anyone had any thoughts in that area.

For instance, we were concerned with the requirements that exist today, and perhaps having a presentation on that score by the appropriate NRC Staff members, and decide what

300 7TH STREET, S.W., REPORTERS BUILDING WASHINGTON, D.C. 20024 (202) 554-2345

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

modifications we might wish to consider and recommend in those requirements, and that could come out of a sequence of activities such as today's, which might be added to our future programs -- our future meetings.

For instance, in the area of design review of proposed plants, how detailed an analysis is conducted by the NRC Staff? Of course, we don't know the answers to these questions from the viewpoint that we have not been immediately involved in them, but we could very well initiate our efforts beyond today's meeting by asking appropriate NRC Staff members to come and make presentations in these hearings.

What criteria are used to evaluate proposed designs? And if we knew initially and this kind of discussion with Staff members, we might very well have some input to their activities, or if there are areas of question that develop in the course of such presentations, schedule efforts in the future.

Among other things, for instance -- and you will hear today from Dr. Bickel when he presents the results of an LER analysis which he made in the course of the last year or so -- that the diesels as an emergency supply of AC power have had deficiencies, and I would like to suggest the thought that maybe we would like to hear a story from members of industry who are associated with fuel cell development. I doubt myself whether fuel cell reliability is yet at a point where it could be acceptable as a substitute for diesels, for onsite AC supply, but I wonder how you would feel collectively about the thought of perhaps launching an investigation to the extent of having a presentation by the fuel cell development people as to what the nature of the beast is as they presently see it, and whether or not there are any gauges for reliability of service for this kind of emergency source.

This kind of question is, I realize, perhaps in an area of specific equipment and facility development, and perhaps I am beyond the purview of ACRS, since we don't design power plants. But it might very well initiate some thought on the part of those who do, on the potential merits of such an application.

It might also serve as an initiative to generate some active pursuit of such sources from the viewpoint of research activities.

I thought, too, that maybe in the course of our future activities, we should hear -- recognizing that the collective concern of ACRS is the reliability of AC power, both offsite and onsite, and its sustained availability -- we should hear from industry members and industry representatives, for instance, from one of the utilities which is well versed with experience in nuclear power plant design and operations, as to what their concepts are of a more reliable AC/DC source of power within a substation -- within the generating station. Whether or not, for instance, they are unhappy with today's diesel and what they might suggest in the way cf improved availability.

Similarly, architect-engineering organizations could be solicited for such comments.

I was wondering, to outline a program for future activities, my letter of August 8th has this kind of thing delineated in fairly detailed words, and I would invite, if you will, collectively, any suggestions you may have, either today or subsequent to today, so that we might structure our future meeting activities.

And at this time I would solicit any comments you would have in this area, or relative to today's activities.

MR. EBERSOLE: Mr. Chairman, to keep this in perspective, I guess we should all be reminded that we are working on part of a larger problem here, and to the extent that we work on this, we are attempting to prevent the failures which are presently visualized in the present AC/DC systems in the narrow context of that particular phenomenon.

As you know, the stations now -- and I think Mr. Epler might have some observations about this later -- include dedicated systems for reactivity control, the scram system. They include dedicated systems for LOCA mitigation. I am referring now to mitigate.

We have, however, mixed systems for shutdown heat removal functions. These are in the plant in miscellaneous

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

arrays and subject to all kinds of industrial accidents that you can imagine. Yet at all times when the plant is in some sort of disarray, as a result of this, this system must be infallible in removing shutdown energy.

Not only is the electrical part of the plant involved in this, but also the piping, the pumps, chemical aspects, and so forth.

We can work to some avail, but not very thoroughly, at just patching and curing the lack of dedication to the shut-down heat removal function by working on the AC/DC systems. We will be, in doing that, working in the prevent area. It is very hard, and it is impossible to ever achieve a degree of adequacy in this area, without stooping over into another part of the world called the mitigate world, and separately considering the mitigate function in the comprehensive sense, not just in the sense of improving AC and DC system reliability, although there would be aspects of this problem in that mitigate area.

So I just want to say here that whatever we do today, we should keep in mind in the background, anyway, we are attempting to prevent. We are likely to fail. Problems will remain after we work as hard as we can at this. We are obligated to step over into the mitigate area to consider what to put in a system for reactivity control and LOCA mitigation; namely, those dedicated to post-shutdown heat removal.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. RAY: Jesse, you bring up some interesting points. There has been no restriction or restraint placed on the activities of this subcommittee in any way, up to the present time, that would restrain us from going into mitigation, as well as conceiving prevention, and the only restraint I would see -- and this is, let me say, an early reference to your memorandum to me -- is that we are concerned with AC and DC power system reliability.

Now I might just as well get into this now. I had a few words with Ep this morning before our meeting started to survey your reactions. Ep has written a memorandum -- I think you have copies of it -- which emphasizes his prolonged concern over the many years, I gather, of activity and consultation to the ACRS and its subcommittees, with the lack of a dedicated residual heat removal system.

He has felt for a long time, and he touches on the point you just made, Jesse, that there should be a dedicated heat removal system. It is not involved with any of the routine standard day-in and day-out plant operation, if you will. It is sitting there as the parachute to use when you have to leap, and it should be tested and so on, to ensure its availability when you have to leap.

My initial reaction to this memorandum was while it is a very, very well justified and meritorious suggestion, it is not within the purview of this subcommittee, but I would like to be in a position, if it is the consensus of the subcommittee, and I would like to mention this later to Bill Kerr when he is here, to recommend to the ACRS, the full committee, that pursuit of this suggestion be picked up and given some type of priority and it be assigned to a specific subcommittee, ad hoc or otherwise, or be, if you will, assigned to us in an extension of our areas of responsibility, to definitely get busy on it, and examine it, and make some kind of recommendation to the NRC Staff, so they make a task out of it. And that we pursue this suggestion to a conclusion of some sort, either an endorsement and specific action, or a rejection of it.

It shouldn't have been let drag the way it has been. I submit that the events that have developed within the industry in various plants would emphasize the importance of a dedicated residual heat removal system.

I am not in a position to say it is sufficiently meritorious to be a requirement in plant design, but I think this thing should be either actively pursued to the point of either killing it or putting it to rest that way, or promoting a specific recommendation to the Staff.

Now, have any of you any comments or feelings to the contrary?

MR. MATHIS: No, I don't have any comments to the contrary, Jerry, but I think, hopefully before the day is over, we will hear enough that I am sure there are some specific items in the area of prevention, many of which Ed just pointed out before, and all of these things do tie together, as Jesse has pointed out.

But I think we do need to get on with the longer-range program of where do we really think we ought to go, but I think we can't overlook the fact that today there are some needs that are being satisfied.

You mentioned the deficiency in diesel generating units, and here again I think most of that is probably a poor maintenance program. The failure on battery systems. Again, poor maintenance program.

But there are a lot of things that need to be done to straighten out today's worry, and then we will move on, and hopefully get to something better tomorrow.

MR. RAY: I think your points are pertinent, Bill. The presentation on the study that we are going to hear today on the probability of, an assessment, if you will, of the DC power supply emphasizes the need for maintenance in the specific DC supply area, and we have had others, too, and I think you will find today's presentation by John Bickel on the OER analysis this afternoon, several of the things you have brought out. And, again, they are things, specific items to which we can address future attention and activity, and recommendation, perhaps to the ACRS.

Did you have any comments, Walter?

MR. LIPINSKI: I was in agreement. I haven't had the opportunity to see your August 8th memo prior to the meeting; but in terms of what the Staff reviews should be covered in Chapter 8 of the Standard Review Plan on Electrical Systems, to see what their outline consists of, on looking over an applicant's submittal, and it may pay for the subcommittee to listen to the Staff as well as look and see what the Staff has recorded in their review document.

MR. RAY: Do you feel that maybe this should be an early activity by the subcommittee, that we solicit and request presentations by the Staff in this area?

MR. LIPINSKI: I think it's important.

One of the other things that comes out of looking at this material that's presented is the single failure criteria has always been used as a good approach to the design of systems. But as I said before, two bad performers don't necessarily add up to an acceptable system. When we look at some of these numbers, particularly after reviewing LERs, we become keenly aware that there are still troubles, if we can believe the numbers that have been developed, in terms of the overall reliability of these systems. So that somehow the single failure criteria has to be extended and some type of a goal defined in terms of what constitutes an acceptable system.

The single failure may not be sufficient. With single failure, all you do is get two redundant systems. It may

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

take more than redundant systems to get us to a desired goal.

Also, looking in the document, I became aware of the fact that in Sequoyah, reference is made to the fact that they have four battery systems, but these systems are shared between the two plants. The diagrams are not presented here to show how that sharing takes place, and the analysis presented here, the buss tie-breaker is an Achilles heel, and presents problems by having been provided for under the design.

I suspect that if one looks at Sequoyah, you will probably find further problems in trying to share four batteries between two plants, in the switchings that are provided for by design.

MR. RAY: It's hard to provide back-up, if you will, with redundant systems, without having interties of some sort.

MR. LIPINSKI: That's right.

MR. RAY: If not impossible.

MR. LIPINSKI: The buss tie-breaker is minor compared to what we see in Sequoyah, if we looked at their detailed single line drawings.

Your suggestion about the architect-engineer is a good one, because that's primarily where these designs evolved from. I'm sure the nuclear steam supply vendors don't even look at what the architect-engineers are proposing, and you see a variety of different designs.

On the subject of residual heat removal, we have had

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

the discussion with BWRs, looking at the event trees that were developed here. You have a choice as to how you develop a tree, depict the events on the BWR. If you pick loss of offsite power and you pick loss of onsite power, you are led to a coremelt as a direct path.

But the way these diagrams are presented, it looks like you are going through several sequences. But it turns out the final element in the residual heat removal are all AC drives. The GE system has turbine drives in some of the other subsystems for high pressure injection, low pressure injection. But the final residual heat removal systems are totally AC-dependent -- well, DC for switching, but the mode of power is a source of AC. And without the AC, I believe the number was in two hours, the system can be expected to be in trouble.

So that the broader question of dedicated residual heat removal systems and what their requirements should be is very important for the ACRS to address.

MR. MATHIS: Mr. Chairman, there is one thing I forgot to mention earlier, and that is that Jesse mentioned that this overlaps into a lot of other things, and I think the whole subject of ATWS is another one that is closely intertied, and we have to keep in mind whatever we decide or whatever we want to recommend.

MR. RAY: Yes, I think your point is good, Bill. We are restricted to the AC/DC power aspects, but we can help

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

recognize and be oriented, if you will, and relate whatever we do with the thermal problems, if you will, the ECCS systems and so on.

And so from this viewpoint, we can't sit on an island and not recognize the waters that are flowing around us.

Okay. Well, now, what I would propose to do personally -- and we will end the day's activities with another discussion of the nature of that which we just had -- is prepare an outline in terms of specific meetings, if you will, a meeting devoted -- and it will be numbered sequentially, two, three, four and so on -- specific areas of concern and presentations by Staff or others, and people in the industry in areas and on subjects that are listed at least for preliminary purposes in my memorandum of August 8.

So if you have any comments post-today's meeting, I would appreciate receiving them, because I will then factor those influences into those proposed outlines, and these will be sent to you, so that you can chew those over and decide what merit they may or may not have, and suggest changes in them, so we will have a more specific program, if you will, for our future meetings and beginning probably some time in February.

My own reaction is that while this is an ad hoc subcommittee, it is going to be in active operation for a fairly long period of time, because there are certainly meritorious problems -- meriting this whole effort and consideration in this

T.2

area.

Okay, has Mr. Fitzpatrick appeared yet?

VOICE: No.

MR. RAY: Okay. Well, suppose -- it seems, perhaps, a little bit early to have a break after having been in session for 25 minutes, but suppose we might take a break now until Mr. Fitzpatrick of the NRC Staff appears, and then we will proceed with the second item on the program which is a presentation of regulatory program and outgoing evaluations and discussions of work planned for the future.

(Recess.)

MR. RAY: May we resume our session, please.

The next subject of concern this morning is a summary of present regulatory policy and ongoing evaluation and discussion of work planned for the future presentations by the Staff.

The principal presenter will be Mr. Robert Fitzpatrick. I understand Mr. Faust Rosa has some introductory remarks he would like to make.

MR. ROSA: I am Faust Rosa, presently Acting Branch Chief of the Power Systems Branch.

First I want to apologize for being late. We had transportation problems this morning. The presentation for the Power Systems Branch this morning will be made by Bob Fitzpatrick, as the Section Leader in the Branch.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

We expect to cover what the present regulations are that we use and reviews of electric power systems, what the guidelines and criteria are, what the present activities of the branch are, and what we propose in the future for revision of criteria.

Without further ado, Bob Fitzpatrick.

MR. FITZPATRICK: Good morning.

I would like to just present a brief summary to you of where we are in AC/DC power systems.

The first slide I have here ---

(Slide.)

-- just shows the regulations that address power systems. GDC 17, which is really the mainstay of the requirements for a power system; GDC 18, which goes hand in hand with the testability of power systems; GDC 5, which covers multi-unit sharing.

We are specifically interested in it in terms of power systems, but that goes across the board for anything that might be shared between multi-units.

In Part B here, I have listed of lesser significance GDC 2 and 4 are protection from natural phenomena, environmental and missile design bases.

These again, the first five GDC, apply across the board to all systems, and parts of GDC 2 and 4 that apply to power systems basically are taken care of in terms of environmental

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

qualification requirements.

I'm sure most of this is of familiarity to the --

MR. RAY: Question, Mr. Fitzpatrick:

Your assumption is, I think, a little bit erroneous, and while we may not have time today, do I understand -- and maybe Dr. Lipinski can help me here -- that these are components of Chapter 8?

MR. LIPINSKI: No, the GDC are part of the federal regulations. The Chapter 8 is part of the STR -- SRP, Standard Review Plan.

MR. RAY: Is there a tie between the two?

MR. LIPINSKI: Well, these, I think, have the letter of the law, where the Standard Review Plan looks to see whether these have been implemented.

MR. RAY: Okay. This clarifies my confusion, and I think, too, in the future, we would like, and I wonder if you would be the agent to do it, a discussion of the Standard Review Plan? Would that be part of your purview?

MR. FITZPATRICK: We certainly could bring a discussion to the committee.

MR. RAY: You wanted to give us just a few words on the area of activity or concern that is addressed by these particular elements. For instance, like the GDC 17, electric power systems, doesn't tell me very much. Can you give me a couple of statements as to the area, of the depth of concern that

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

the regulation touches in this particular area?

MR. FITZPATRICK: General Design Criteria 17 requires an onsite and offsite power system.

MR. RAY: And the characteristics of those systems are addressed?

MR. FITZPATRICK: And it lays out the basic criteria for them.

And then my next slide --

(Slide.)

-- is what the Staff has put together in terms of explanation and amplification of what is required by this.

MR. RAY: Okay.

MR. FITZPATRICK: My main purpose in showing this slide was to show that these are the regulations.

The next slide is what the Staff has done to try to implement them. I have labeled this one "Established Criteria and Guidelines." I have taken most of this out of Chapter 8.1 of the Standard Review Plan. It's a list of the basic regulatory guides, some of which reference IEEE standards that the Power Systems Branch uses in its review of power systems.

For the reg guides, we start with Reg Guide 1.6, one of the very early reg guides, and it deals with independence between redundant power divisions and the requirements of this regulatory guide center around a prohibition of things like swing busses where you could have loads tied to one safety

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

division, and given a loss of power or some fault, you would automatically switch over to another division.

Our concern here is that you may take the fault of the problem along with you, and so the regulatory guide prohibits designs of that nature.

Regulatory Guide 1.9, also another early reg guide which has just recently been revised to reference IEEE 387, deals with --- it deals with diesel generator capacity and requirements for the diesel generators.

Regulatory Guide 1.32, which is an endorsement and references IEEE 308, this is the basic document dealing with Class 1E electric systems. This is equivalent to the reactor protection systems of IEEE 279. This is one of our most basic documents.

Regulatory Guide 1.75, which is an endorsement with comments of IEEE 384, physical independence of electric systems. This deals with minimum separation requirements of a power system.

Regulatory Guide 1.81, which is really a carry-on of GDC 5 multi-unit sharing, talks about sharing of onsite power sources between multi-units. This is a practice in the early stages of nuclear power that was allowed and was used. This is no longer permitted. We don't allow sharing between units of AC or DC onsite power sources.

MR. LIPINSKI: Excuse me. On that point, where does

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

the Sequoyah fall into this?

MR. FITZPATRICK: I'm really not sure where that fits in. I'm also not totally familiar with the Sequoyah design.

MR. LIPINSKI: The report we have here says Sequoyah has four batteries that are shared between the two units.

MR. ROSA: If I might interrupt, when Bob states that sharing is no longer permitted, he means that under the regulations or the way we have interpreted them and applied them, sharing is permitted in plants that are in the OL stage now, but whose design was finalized before we issued this reg guide.

You can't make these changes when the equipment has been purchased, and the system design is essentially in concrete.

MR. LIPINSKI: That's what I was asking for, the date when your change had taken place. Effective when?

MR. ROSA: I don't recall the date. It would be a matter of months after the -- if the construction permit had been issued, up to a matter of probably six months after the issue of the reg guide. But I don't have the date of issue of the reg guide.

MR. LIPINSKI: Okay. Thank you.

MR. FITZPATRICK: I believe it's somewhere around 1976.

The other thing I might mention regarding that, if we come across a design that does pre-date the requirements of regulatory guides, to have total separation of onsite power sources, that still doesn't relieve the design from being equivalent -- there are also wordings in the guide that you should not allow sharing of the power sources to provide any less capability or capacity than would be provided if you had separate power sources dedicated to the units.

So in the Sequoyah design, the concern would have been the battery size, how to handle two units. Each of the four batteries would have been spread across.

MR. LIPINSKI: As we get into this later, we will find there are certain features compromised based on the design and being allow to swing these batteries between units. I suspect we will see further compromise exist.

MR. FITZPATRICK: That's also why the Staff has come up with a regulatory guide to try to get away from any possibilities in this area.

The next regulatory guide of interest to the Power Systems Branch is Regulatory Guide 1.108, periodic testing of emergency diesel generators.

We have been implementing this guide since, I believe, about 1977, and it requires an upgrading of diesel generator testing requirements prior to the regulatory guide, and then its subsequent placing into the state of technical specifications.

Diesel generator testing was done on a staggered basis once every 30 days, and that was independent of what the failure rates might have been.

The regulatory guide now has taken the position that you look at your last 100 starts with the diesel generators, and from that you can get a demonstrated reliability of the units.

The goal of the regulatory guide is to have a reliability of 10^{-2}. That's one failure in 100 starts. If, when you look back over your last 100 starts, you find that you have a failure rate in excess of this, the regulatory guide then says you start testing on a more frequent basis. With two failures, I believe it's 14 days; three failures, seven days; and four or more, you are down to a three-day testing interval.

Our hope here is to shake out any generic problems that may be in the machines, and also this has the effect of ensuring that the maintenance on these machines really gets top priority because certainly utilities don't want to be testing these machines every three days, if they can help it.

So that's where we are with that regulatory guide --

MR. RAY: Question:

This appraisal of performance is based on each machine, or the collective aggregate of all the machines in the station?

For instance, there's 100 starts of all the machines, or is it 100 for each one? Do you see what I mean?

MR. FITZPATRICK: Yes. It's each individual machine, and once you get to -- no, it's the other way around, excuse me.

MR. RAY: It's the system?

MR. FITZPATRICK: Yes. And the testing is also on a per-station basis of all machines that go into the testing program every 14 days, every seven days.

MR. RAY: It's an appraisal of the aggregate system?

MR. FITZPATRICK: That's correct.

MR. ROSA: Excuse me. To make that clear, the 100 tests incorporates all the tests on all the diesels per unit. That's all the diesels assigned to one unit. The test frequency applies to each diesel.

In other words --

MR. RAY: I understand. Each component of the system.

MR. ROSA: Right.

MR. DAVIS: Excuse me. Could you tell me if these tests include tests of the automatic startup part of the system? And do they include having the machine assume the electrical load that it is designed to assume?

MR. FITZPATRICK: When you get down to a three-day test interval, what is required by the current technical specifications would be that you would be allowed to manually stop the machine and load it up to maybe 50 percent of its load; something like that. So you are really just trying to check out the machine. On the 31-day interval, which would be the normal interval, if you are maintaining a 10^{-2} or better reliability, you would stagger the testing on the diesel. One

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

time you start it manually, the next time you might start it with a safety injection system, the next time with a loss of offsite system signal. And the refueling outages not to exceed every 18 months. You would go through a full system test.

Regulatory Guide 1.128 is an endorsement of IEEE 484, installation design and installation of large lead storage batteries, and this is coupled with Regulatory Guide 1.129, which is a reference for IEEE 450 on maintenance testing and replacement of large lead storage batteries.

We will be getting into batteries in DC systems a little later in the program, so I didn't plan to say much more about that.

The next two items, B and C on the list here, talk about the Millstone event in '76, which was the degraded grid voltage problem that they had, and the Arkansas event in 1978, which among other things showed us an inadequacy in their station distribution systems.

These two events the Staff has come up with positions on, and we have gone out to all the operating reactors and to all the reactors in-house under a licensing review, and have required all of them to meet the Staff positions on these two subjects.

We are still in the process of evaluating operating reactors. This is being done under our technical assistance contract with PG&G and Lawrence Livermore Laboratory.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

We expect to fully complete all of the operating reactors, checking them for both events, and how they meet the Staff positions, and be able to sign off on that acceptability within, I would say, no later than six months from now.

This has been a long haul on this particular subject, but we are near the end of the time on it.

MR. EBERSOLE: Going back to 1.6, I would like to have you go to the roots of what you regard to be redundant divisions or systems and how you expect to meet accident situations at the plant, because there is some confusion about what really constitutes redundancy. How do you define redundancy?

MR. FITZPATRICK: For the power system, what we are requiring is a split buss concept. If you would draw a one-line diagram of the system, you could see all of division one busses, for instance, would fall on one side of the paper, and all of division two on the other side of the paper. And there would basically be no interconnections between them, and either division would have the full complement of equipment necessary to mitigate the postulated events on safety --

MR. EBERSOLE: Either one?

MR. FITZPATRICK: Right.

MR. EBERSOLE: Ordinarily when you talk about redundant divisions, you say I have redundant capability to meet accident circumstances, if either of the two divisions fail, and I will still be competent to deal with that.

There's a subtlety here in such systems as the one we are going to discuss later, DC systems, and the failure of one of the redundant systems in the beginning precipitates an accident in its own right. Therefore, you must subsequently meet a complicated situation without redundancy. You therefore have no capability to meet a complex and dangerous situation with the benefits of redundant configurations after the accident.

Do you follow me?

MR. FITZPATRICK: Yes.

MR. EBERSOLE: Is it your interpretation that that is a satisfactory statement of affairs, if the first system fails and precipitates an accident, and thereafter you must deal with it in a single configuration?

MR. FITZPATRICK: No, but that's one of the things we are attacking here with the DC power system.

MR. EBERSOLE: There are many other systems like that, service water, et cetera, et cetera.

MR. FITZPATRICK: But in terms of the power systems, I don't see the analogous event in the terms of the diesels, the AC part of the system.

MR. EBERSOLE: No, that doesn't apply because you have offsite power for that.

MR. FITZPATRICK: Even then, there should be the interaction of a diesel doing something that would cause a nuclear incident of some kind.

MR. EBERSOLE: Well, I would hope that you would someday set down a clarification of what you believe to be redundancy in this context that I speak of, where the failure of the first redundant one precipitates an incident in its own right which thereafter, in the present rationale, you must deal with in single configurations.

MR. RAY: Jesse, are you pointing out that perhaps in a virgin state, redundancy would require redundancy within redundancy?

MR. EBERSOLE: It would require it to meet it in abnormal situations.

MR. RAY: So that when you lose a track, it has a back-up?

MR. EBERSOLE: Yes.

MR. EDISON: Could I interject a comment here?

What you are saying here seems to be more of a philosophical approach to safety, and not strictly electrical-oriented.

MR. EBERSOLE: That's correct.

MR. EDISON: Any system that has a two-train system

MR. EBERSOLE: Which is on 100 percent demand all the time, not just occasional demands, for circumstances which are extraneous to the system itself.

MR. EDISON: I wanted to clarify that's a general philosophy.

MR. LIP?.SKI: I think what's important to that is the initiator. This system could fail silently, and it would not represent a challenge, but if it fails and precipitates the chain of events, that is an important consideration.

MR. EBERSOLE: I know of no system which doesn't precipitate some degree of emergency. Some systems produce worse effects. The worst of these is DC.

MR. ROSA: If I might interject, also, as of right now, the criteria require that electrical systems meet the single failure criterion. That's the DC system I am talking about, and we regulate to that. The objective of this DC reliability study, as it's going to be discussed later, was to evaluate whether or not those criteria were adequate or needed to be revised, and I hope perhaps we can get closer to that objective at the end of that discussion.

MR. DAVIS: I have a related question to that:

Does the so-called minimum system that was analyzed in NUREG 0666 meet all of these requirements and would be licenseable against these requirements?

MR. ROSA: May I answer that?

The minimum system evaluated in 066 -- NUREG 0666 does meet all of the minimum requirements. However, it has been quite some time since we have reviewed a plant that did not considerably exceed those minimum requirements.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. EBERSOLE: Don't you find it unusual in this particular aspect that you find industry, by and large, in fact exceeding the minimum requirements on a matter of its own good judgment? It's strange to me the regulatory process wouldn't be even more conservative than they are.

bu2

MR. ROSA: Well, you know, safety is really the Applicant's responsibility. Now they exceed the requirements not only for safety reasons, but for economic reasons. They also exceed these requirements because throughout the existence of the NRC, electrical reviewers have been urging them to exceed these requirements, and there is an inherent difficulty within the NRC in changing criteria. And so in a course of licensing reviews, when we find we are getting what we want, really, even though it exceeds requirements, we leave well enough alone, and eventually given the time, we are going to revise the criteria to include what we are already getting in excess of present requirements.

end 2

MR. FITZPATRICK: That is just some background as to basically where we have been.

I would like to discuss briefly with you now where we are today, some of the things we are thinking about and pursuing today.

(Slide)

The first item on this list, backfit of Regulatory Guide 1.108 to operating reactors, as I mentioned previously, I believe it was 1977 when the regulatory guide came out. We started applying it immediately to all those reviews that were in house, either CP or OL.

We are now in the process of attempting to get the Division of Licensing and the Division of Systems Technology, who have control over the standard technical specifications, for the three of us to work together to bring the old plants into conformance with the provisions of this regulatory guide.

One of the problems we have found in doing many of our studies, and you will probably hear about that later today, is we are just not sure what the failure rates on some of these diesel generators are. Most of the diesel generators are at their operating plants. We haven't had what we believe are strict enough requirements on reporting. So we go back and look at a plant's history, and we are not sure if we have got all the attempted starts and the data base to try and figure out a failure rate.

Another attempt of Regulatory Guide 1.108 is to give us an accurate data base on exactly what is happening with the diesel generators, so we are pursuing right now trying to update the technical specification of all the operating plants to come into conformance with the provisions of this guide in terms of testing, reportability, its definition of what is a valid and invalid failure, and all the rest of it.

We are also working with the Standard Technical Specification people on a newly formulated set of battery technical specifications. We have had a member of our branch working closely with an IEEE subcommittee to try and make the technical specifications for batteries and DC systems to more accurately reflect what is really going on with them.

Our previous requirements have been that if you measure the specific gravity of a battery and it might be one point less than an arbitrary cut-off, we declare the battery inoperable. Well, that gives a plant essentially two hours to either fix it or start shutting down, and we all realize that there is still a lot of capability left in that battery. Just how much, we may not be sure of, but we know there is quite a bit still left if you are only one point below the cut-off.

MR. ROSA: That is the specific gravity of the pilot cells, the two or three cells Bob is talking about. That doesn't reflect really the overall condition of the battery with regard to specific gravity.

MR. RAY: Question. However, once these pilot cells are designated, they remain pilot cells. You don't swing them around, do you, from one cell to another?

MR. ROSA: They don't do that between tests. They may do that later on, you know, in a year or so, at yearly intervals or so. The ones designated, they remain pilot cells for a considerable length of time.

MR. RAY: But that swing service, if you will, is their option; it is not a requirement.

MR. ROSA: I cannot be sure, but I believe it is their option, yes.

MR. RAY: It would seem on the surface of it that a better test of a battery would be varying the pilot cells over a period of time so you are not following the history and characteristics of one cell, you are getting more representation of the total battery.

MR. ROSA: Even in the old technical specifications the specific gravity of all the cells had to be measured every three months. The pilot cell measurement is every seven days.

MR. RAY: In today's specs?

MR. ROSA: And today's specs also include that. In fact, I think Bob can go into a little more detail about what the newly formulated tech spec requirements are.

MR. FITZPATRICK: One of the added features of the new tech spec requirements would be that in your seven-day check of the pilot cell, if the specific gravity is low, if you determine it is low, you immediately do a couple of things.

You first check all the other cells to see where they are so you have an overall understanding of what shape the battery is in, and if the average of all the cells is -- I'm not quite sure of the point differential here, but if it is at least close to what it should be, even though you have one or maybe two low cells, you are allowed to proceed with operation while trying to correct the low specific gravity for the next seven days if at the same time you verify that you are receiving less than 2 amperes charging current.

This is what was worked on with the IEEE. The idea behind this is that if you are not really charging the battery to any great extent, there is a confidence level there that the battery has a sufficient charge in it, should something come up, to get you through the event. That is the philosophy behind that.

MR. EBERSOLE: Is there a criterion today that requires that the apparatus connected to the DC busses must sustain, must resist the levelizing voltage level to overcome random charge rates in the batteries without disconnecting those loads and transferring them to another source while you levelize?

MR. FITZPATRICK: No. The requirement as it stands right now is that if the loads are not capable of withstanding 130 or 140 volts --

MR. EBERSOLE: You allow that condition today?

MR. FITZPATRICK: Correct. That is still allowed.

MR. EBERSOLE: Do you intend to do anything about that?

MR. FITZPATRICK: I don't know of anything.

MR. EBERSOLE: If you don't, what are you going to do to avoid disconnecting the battery and performing a number of switching functions in order to get the battery levelized?

MR. ROSA: If I may interrupt, I believe that the equipment connected to the DC busses is all supposed to be able to withstand battery equalizing voltage.

MR. EBERSOLE: I understand that is not the case.

MR. ROSA: That is, I believe, where we have had problems, where the equalizing voltage used was greater than the voltage capability of the equipment.

Now, it is true that normally equipment is rated plus or minus 10 percent as far as voltage is concerned.

With a 125 volt DC system, you would be able to withstand 135 volts continuously. You can perform equalizing charges at that voltage or ev slightly below.

MR. EBERSOLE: Do you require that be done?

MR. ROSA: Not specifically. If it has been brought to the attention of all operating plants --

MR. EBERSOLE: It takes longer.

MR. ROSA: It takes longer, yes, and in some instances where there are tie lines between batteries in a two-unit plant, for instance, like at Zion, they do disconnect the battery while applying an equalizing charge and connect a bus to a battery in the other unit. So that is being done.

MR. EBERSOLE: Thank you.

MR. FITZPATRICK: I think a portion of the answer to your question would be coming a little later in the presentation.

The next item, C, is NUREG/CR-0660, which is diesel generator reliability. This is a result of the study by the University of Dayton where they examined the operating history of diesel generators of the plants and came up with a number of specific recommendations to help improve long-term reliability of these machines.

We have immediately taken the recommendations of this NUREG with only a couple of minor exceptions that we didn't feel applied, and we have gone to all the plants in house for review, CP and OL, and required of these plants to demonstrate how they meet these recommendations or why they should not and what they have done that would be equivalent.

We are also in the process now of interacting with the Division of Licensing and Division of System Safet Technology to attempt to apply this same set of recommendations to the operating plants to see how those out there stack up against these recommendations. That is ongoing at the moment.

Item D here, Task Action Plan A-25, dealt with nonsafety loads on Class I busses. The idea behind this Task Action Plan was we had a question in our mind whether the requirements of Regulatory Guide 1.75 may have been too stringent in terms of requiring a total separation of nonsafety loads from Class I busses and not giving any credits for fault-interrupting devices.

So we had Oak Ridge National Laboratory do an independent study on this to determine whether or not we were indeed too conservative. We have a preliminary report from them that, unfortunately, has set idle in someone's "Hold" box along the way here due to other things, basically since TMI-2. We haven't had time to really check back into this.

The reason we haven't gone out of our way to get back into it sooner is the fact that it is in a conservative direction in terms of are we too strict or not. From preliminary analysis of the report from Oak Ridge, we don't think we have been too strict. We think we are probably pretty much where we should be in terms of requiring the separation of the non-Class I loads from the Class I busses.

Hopefully we can finalize something on that in the not-too-distant future and update the Standard Review Plan to reflect this, but as I say, from our preliminary look at the report from Oak Ridge, we don't think we have gone overboard in our conservatism, so that we haven't really tried to hurry this up.

The next item on the list, inverters, is an item that has come up rather recently. There have been a number of events at various plants that have caused upsets of varying magnitudes. We are in the process right now of doing a preliminary study on this.

There was a paper recently presented to, I believe it was, Commissioner Bradford put together by a group in the Division of Licensing where he had some direct questions on inverters and their role in some of the events that occurred.

The Division of Licensing right now is working on some specific areas that are associated with the events that occurred, and in a more generic sense, the Division of

Safety Technology right now is doing a study -- that LER Review Group is in the Division of Safety Technology -- is trying to do a broad study on exactly how much of an observed problem this is; and from that point, when they make that determination I expect some kind of action plan will be created to further delve into the inverter problem.

Task Action Plan A-35 on adequacy of off-site power systems. We have in house now a final report from Oak Ridge National Laboratory. They were the contract consultants that provided the technical assistance on this particular item.

It was a many-faceted task action plan. Part of it was degraded grid and items like that which we have taken actually out of the task action plan and are almost fully implemented. The remainder of the results of this study we intend to provide to the Office of Research in their dealing with Task Action Plan A-44 on station blackout.

MR. LIPINSKI: Does that analysis include the recent four-state blackout out west that extended for over 24 hours, I believe?

MR. FITZPATRICK: No, this study has been in house quite a while now. This is another one that has had to take somewhat of a back seat this the Three Mile accident to try to cause a trade-off for what we felt were more important things.

MR. LIPINSKI: So the latest data point will not be in that.

MR. ROSA: If I may interrupt, I believe that study is based primarily on the blackouts that occurred in Florida over the past few years.

MR. FITZPATRICK: It specifically analyzed some of the major Florida events of '77, '78 and the major event in New York City.

MR. LIPINSKI: Florida is a little unique, being a peninsula, but I was surprised to find that four states out west that should have been intertied went black simultaneously.

MR. FITZPATRICK: Another identified generic item, TAP B-53 generator circuit breakers, is active in the branch right now. The McGuire units were the first operating licensed plants to come in with a generator circuit breaker, and the purpose of the generator circuit breaker was to give immediate access sources to the on-site emergency power system without using actually start-up transformers.

The McGuire system uses only two transformers, and in order to do that you have to be able to guarantee you can isolate the generator from the system even under fault conditions. So the McGuire design was the test case for us on exactly what we would require in terms of demonstrating the capability of these new very high current interrupting devices.

We hired a consultant on this and he provided us with an independent review of the McGuire design. I am not sure if the ACRS has fully reviewed all of that yet or not on that particular aspect of the design, but we feel that with our consultant's input we are in a position to formulate a branch position.

The reason we haven't rushed into this -- this input is also probably four years old. We haven't rushed into it because it doesn't affect any operating plant whatsoever and we haven't run across another plant coming in for an OL review that uses a generator circuit breaker.

So right now we are between having the input required to create a branch technical position, and at the moment we are in the process of creating that technical position to update our standard review plan. We are in the process of updating the standard review plan right now and we plan to include this technical position in our update.

There is also work by the Office of Standards Development on a regulatory Guide on lightning protection. This is a draft guide. I understand we will be coming down to ACRS in February for review.

MR. EBERSOLE: Does this include implications of the now expanding use of miniaturized solid state equipment in safety circuitry which is spiking?

MR. FITZPATRICK: This regulatory guide?

MR. EBERSOLE: Yes.

MR. FITZPATRICK: I don't believe so, no. We are picking that up in Item J on my list here.

MR. EBERSOLE: Okay.

MR. FITZPATRICK: In terms of TMI Lessons Learned for the power systems there really wasn't any specific lessons learned on the TMI-2 accident dealing with the power systems.

In the Lessons Learned group that was formed after the accident, the only items that they determined were associated with the power system was that they required that PWRs have the capability of providing an on-site power supply for pressurizer heaters and that the PORVs, block valves and pressurizer level indicators should also receive uninterruptable backup power from an on-site system.

The review of those on the operating reactors was implemented by task forces shortly after the Lessons Learned came out, and we are applying these two requirements routinely to the reviews in house.

MR. LIPINSKI: There was one lesson learned on TMI pertaining to the diesels. It initially started as part of that accident and they had to be manually tripped but they were not reset. If I recall, they set in the condition for the order of one hour. Had they had loss of AC power, the diesels would not have started from the control room. An engineer walked in at one point and noticed their condition and told them to reset them.

They put their electrical switches in the manual mode such that they would come on automatically, but for a period of time they were vulnerable with loss of AC, and I don't know what their time would have been to trace down, open the doors on those diesels and get them started.

MR. FITZPATRICK: That is correct.

MR. LIPINSKI: But nothing has been factored in from that lesson into plants in terms of vulnerability of those diesels to lock them out the way they did?

MR. ROSA: If I might address that, that is an operational error, I am sure. The diesels should be in the mode to respond automatically to a loss of power signal at any time, and the failure to do that was another one of the human errors that occurred, I believe, at TMI. The TMI Lessons Learned do not address that particular item except in the broad context of the human error problems that were revealed by the TMI incident.

MR. LAWROSKI: There is also a question of diesel design as to whether you require complete remote operation of those diesels with respect to the inlet valve control that is manually operated on those particular diesels. There does not appear to be a requirement that that particular function be executed remotely.

MR. ROSA: We don't have a specific requirement for that as far as I can recall, and I really don't feel that it is necessary that this be operated remotely. Most of the time -- in fact, the great majority of the time where you would need to do this involves failures during test where you really don't want remote reset of the capability to respond to an automatic accident signal because the trip may have been the result of a protective trip of the diesel generator which if it were started would damage the die[illegible], and therefore you would like to have a man go down there to the diesel room and look at the enunciator panel down there and make a judgment as to whether this reset should be effected.

MR. FITZPATRICK: Item J up on the screen here is EMP. That stands for electromagnetic pulse. This is the effect of, say, high altitude detonation of a nuclear weapon and its effects on systems. The Instrumentation and Control Systems Branch has taken the lead in pursuing this. It also affects the power systems.

They are in the process now of contracting technical assistance to study the vulnerability of nuclear plants and what might be required to protect them from such event whether it be a nuclear blast or even a systems-generated EMP. That is an act of sabotage or whatever.

MR. LIPINSKI: The subject was before the ACRS about two or three years ago, and the resolution at that time was that there was no requirement on nuclear plants to withstand EMP. Has this position been reversed?

MR. FITZPATRICK: There is still no requirement today for plants to survive an EMP. We are now looking into it in detail to determine first whether or not EMP is a threat, and then what might be done to protect from it. I have very limited personal involvement in this but I do understand that there are devices available today you can buy to plug into your system which do help mitigate the effects of EMP.

MR. LIPINSKI: There are volumes of military reports because they had subsidized all the studies on how to protect military equipment against EMP. The same techniques are directly applicable to nuclear plants.

MR. FITZPATRICK: That is correct. There are means today to protect circuits in the nuclear plant, but this study is first geared to determine if it should and to what extent we should require it.

MR. ROSA: If I might expand on that a little, between '74 and '75 when the issue first arose and the present time, I think for two reasons, the priority of this item has risen. One is the international situation, and the second is the nonavailability of pulse generators which could be used by saboteurs from off site to in effect introduce an EMP-type pulse to the systems emanating from the plant.

Another reason why it is being addressed now is that I believe four or five years ago there were issues of safety importance that far surpassed EMP. Now we think we should get to it.

Now, the objective of this study is this. It is to determine the vulnerability of plant shutdown systems, safe shutdown systems to an EMP-type disturbance either from a nuclear weapon or from an off-site pulse generator.

MR. EBERSOLE: Lightning?

MR. ROSA: Not lightning per se.

MR. EBERSOLE: A minute ago you said you were going to cover the lightning aspects in this study.

MR. FITZPATRICK: No, sir. What I meant was we were going to cover some of the spiking problems in talking about the EMP, not necessarily tying it directly to lightning.

MR. EBERSOLE: I see.

MR. ROSA: I might add in that regard that an EMP pulse is much steeper than a lightning-produced pulse. Therefore, if there are any equipment modifications required to protect against an EMP, they will certainly be more effective against a lightning-induced pulse.

Another objective of the study is to determine what is to be done to protect the safe shutdown systems -- and I am emphatic that it is only the safe shutdown systems -- against a possible EMP event, and then to determine whether further studies are indicated; but there is no intention to at this point go beyond determining the vulnerability of the safe shutdown systems to EMP and determining what modifications need be made to effect protection of this as required and to determine an estimate on the cost of such modification.

MR. RAY: Do you have any idea when the results of that study would be available?

MR. ROSA: The schedule is for completion at the end of 1982, I believe. It is well under way, by the way.

MR. BASDEKAS: Mr. Chairman, may I respond on that? My name is Basdekas. I would like to respond somewhat on the question of EMP.

I believe that the EMP question has not been addressed properly. It probably was by the Office of Nuclear Reactor Regulations -- it is not going to get anywhere for the simple reason that it attempts to focus on a number of systems which have been more or less arbitrarily picked up to designate its priority one, priority two systems, the decay heat removal systems and other systems of equal importance.

As Mr. Rosa pointed out, this will be looked at, if at all, if studies for the systems are indicated at the comletion of this two-year study. I believe this two-year study that is contemplated by NRR is -- the best way I can describe it is an attempt to revamp the wheel, the wheel that has been invented a long time ago by the Defense Department for their military systems.

I don't believe it is a question as to whether or not the safety and other systems or control systems and instrumentation in general for nuclear power plants are vulnerable to EMP. It apparently is a question that this will not answer. It is a question of what steps we should take, and I believe if we demonstrated the approach we have been pursuing for years now, it will be the equivalent of spinning our wheels and buying time -- for what, I am not sure.

But since I cannot read minds, the only thing I can base my comments on is this feeling, and I think it is important to come in and say, to seek details on the subject, on the problem itself, the rationale, if any.

Thank you.

MR. RAY: Thank you.

MR. ROSA: I would like to respond somewhat to that comment. The study will include a review panel which, among other individuals that are knowledgeable in the field, will include officially the Defense Nuclear Agency, which is the Department of Defense agency that is responsible for the protection of military installations and equipment against EMP. So we will get input to this study, the Defense Department background in this protection against this event.

I think Mr. Basdekas has incorrectly described the study itself. The study itself, its objectives and procedures are described in a task action plan, or a task plan, I guess you would call it. It is not called an action plan within the NRC. And as I said before, it will investigate what the effects of the EMP phenomenon is on all of the safe shutdown systems, all of the systems needed to effect safe shutdown.

It will determine, if it is found that these are vulnerable to EMP such that safe shutdown is in question, it will determine what needs to be done to protect the systems, and it will determine an estimate of cost to do so and also what effects these revisions might have on the normal reliability of the equipment involved.

Now, the study was scoped to include only the vulnerability and hardening of the safe shutdown systems in order to make it viable. If you were to consider EMP effects on all systems in a plant and embark on an analysis of such effects, it would be an infinite study almost.

Now, as a final product of the study there will be recommendations with regard to further studies that might be indicated by the results of this study. That is where we are now.

MR. RAY: Mr. Rosa, you have a Defense Department participation. You have the benefits of the results of their studies. You won't repeat those, for instance. You are going to start with whatever those conclusions were, I presume.

MR. ROSA: That is absolutely right. The contractors that are being brought aboard for this study are the same contractors that the Defense Department has utilized in doing EMP work for them.

MR. RAY: So you won't plow over ground that is already plowed.

MR. ROSA: No, sir, we won't.

MR. RAY: The second point. The results will be presented in such fashion that an operating company can measure the import or the consequences or the cost, if you will, of expanding the scope of application. I can see a situation recognizing that companies can if they want to maintain operation, not only shutdown safely when a shutdown is required, but because of the economy of the operation, they want to continue it, so therefore they might very well wish to expand the application of hardening techniques, if you will, to other controls.

MR. ROSA: I would think the final report would include information that could be used in that manner, yes.

MR. FITZPATRICK: The last two items on my list here, K and L are Task Action Plan A-30 and A-44. These are also two items that are keeping us busy these days. I would like to go to the next sheet and just talk a little bit more about them. You are going to here presentations on both today.

(Slide)

What I would like to talk about here just for a minute before we get into the two task action plans is what we feel we are going to do with the results of this study. For instance, on Task Action Plan A-30 that you are about to hear about, part of A-30 involved a sensitivity study.

I am not going to talk too much about A-44 because that is more or less a starting program and A-30 is a finishing program. So similar words will apply to A-44 in its final stages. But I will limit the remainder of my remarks here to A-30.

We are going to look at this sensitivity study analysis that is in the report. We would hope to take the recommendations of the report and apply them to all of the plants, not just those in the licensing process, but to go back with the recommendations that are there and apply them to the operating reactors in terms of creating new criteria for, say, construction permits and maybe even OLs. We will look at the sensitivity study to see what additional benefits may be there that might be pertinent to apply.

Another item we are thinking about along these lines is the fact that, as Mr. Rosa said earlier this morning, the DC designs we are seeing today go far beyond the minimum DC design, which is basically a hypothetical design of the bare minimum system that would meet the regulatory requirements, and that is what was studied in the task action plan as a base design.

Because we are seeing so much more than what is required, we are giving consideration to maybe updating the criteria to meet the input that we are seeing. We also as we go along will be factoring in any operating experience that comes along in finalizing our position as a final output of the task action plan.

Are there any questions?

MR. LIPINSKI: Yes. The operating experience in the reports we have seen before us, even though industry exceeds your minimum requirements, do you conclude that what industry offers is adequate?

MR. FITZPATRICK: You are asking me if I have concluded that?

MR. LIPINSKI: Yes. My question is should you extend your requirements to even go beyond those that industry currently offers to make the systems even better?

MR. FITZPATRICK: Well, we are still in the thinking process right now in terms of Task Action Plan A-30. We are also awaiting the ACRS comments and if any ideas come out of the ACRS that could be carried forward.

MR. LIPINSKI: Your concluding statement was you are thinking of bringing your minimums up to meet what industry offers. You did not extend that statement?

MR. FITZPATRICK: I see. Yes, we are certainly thinking of bringing the requirements up to what we are seeing, and it is also in the thought process of what may be required beyond that.

MR. LIPINSKI: Okay.

MR. ROSA: May I make a another comment here on just exactly how we go about developing new criteria? Under the present NRR organization, a licensing branch, technical branch would first develop branch positions incorporating what it considers to be new or revised requirements. We would expect to go ahead doing that with regard to ECC system requirements and so forth.

Once developed and before it is really applied, this new branch position would have to be approved by the Division of Safety Technology. So there is an overview of what we propose in the way of new requirements by Division of Safety Technology. With regard to applying any new positions to operating reactors, backfitting them to operating reactors or even backfitting them to plants in the licensing process, the Division of Licensing has some input on that.

So it is not something that we can do in isolation. We will initiate the process. This is all I am saying here. Hopefully there wouldn't be any problem in getting concurrence from both DST and DL.

Now, we may skip the step of a branch position if informally we find that there is concurrence among all the organizations involved and go directly to development of a regulatory guide, in which case we would be working with the Division -- or Office of Standards Development, and in which case the ACRS, of course, would be involved in the final approval of any such guide.

MR. RAY: I would like to comment first that it is significant to me that your branch does generate, if you will, a need; you don't wait for some external organization or someone in the NRC to tap you on the shoulder and say, "Hey, look, there's a deficiency here." In your investigations -- you generate these investigations to establish -- in a sense, it is sort of an activity establishing the adequacy of present requirements and take the step by way of initiation to introduce changes that should be made and review those other divisions, if necessary.

MR. ROSA: That is correct. We do that, and we intend to continue doing that.

MR. RAY: I think that is an important point to make for the record, both in the public mind as well as the ACRS mind.

MR. ROSA: Well, I might give you an example that Bob touched on previously, the recommendations of NUREG-0660 on diesel generator reliability enhancement. Immediately on publication of that final report, we developed a branch position and immediately began applying it in the licensing process and without regard to backfit considerations. In other words, any OL that came down -- the next OL that came down, it was applied to that and is being met.

We did do the near-term OLs, which were the ones that this was applied to first. The first refueling period to effect any improvements that needed to be made in order to meet all the recommendations. And I want to emphasize that there were 13 recommendations. I think one in specific to a diesel generator type. And it's only applied to those plants that have that diesel generator.

One we considered not proper. But all the others, we are requiring conformance to those recommendations or a very strong case for nonconformance.

MR. DAVIS: Question, please. I am getting the impression in this presentation that because industry has better systems, the NRC may require more stringent requirements on these on the systems themselves. It seems to me like the criteria should be based on whether or not the plant is adequately safe or not.

Could you explain to me on what basis you are going to decide whether the power systems need to be upgraded or not?

MR. ROSA: Bob, may I answer that?

MR. FITZPATRICK: Certainly.

MR. ROSA. The way we do this is, as of right now, we have to assure ourselves that the designs conform to the regulations. We attempt, where we feel we should, attain designs that exceed the minimum regulations. But in order to make and formalize new requirements, we must have a firm valid basis. In the case of the DC systems, I believe this report of TAP A-30 will provide that basis. In the case of the AC systems I believe that the results of TAP A-44 will provide that basis.

I don't think we can, at this point in the regulatory process, develop new criteria on a qualitative or "gut feel" basis. You have got to have more than that. And the only way to attain such a basis is by means of comprehensive quantitative probabilistic studies involving the complete systems. And this is what we are attempting to do.

MR. EBERSOLE: I hope you mean complete in the context better than completion was done on the ATWS mitigation systems which we now know, as a result of the Browns Ferry incident, didn't even include observation of peripheral systems that grossly affected the operation of the safety systems.

MR. ROSA: I am sorry, I can't respond to that. I am not familiar with that issue right now.

MR. EBERSOLE: Well, I think that is the case of -- it affected the -- it can be done by people who sit in an isolated place and really don't know what the plants are, and they can be done right here in this DC power study. I notice, as a matter of fact, there has yet to be a walkthrough plant on a typical basis as at TMI-1 to look at a two-track system and see what really are the physical interfaces are there which are not covered in this report which was done by Sandia.

MR. ROSA: Well, Jesse, you know, there is a difficulty here. All of these systems are unique as far as physical configurations are concerned -- are unique to each plant. And a study like this attempts to produce results that can be generically applied. And to attempt to go out to plants and try to discover the weaknesses in each plant is an insurmountable job as far as we are concerned. But this we can do as a generic study of this sort and then draw a reasonable engineering conclusion from those results and apply them generically.

MR. EBERSOLE: Don't you think there is an order for an occasional examination for the case in point?

MR. ROSA: We do that. We do that routinely.

MR. EBERSOLE: Have you done it for this case?

MR. ROSA: No, we haven't done it for this case.

MR. EBERSOLE: Was it ever done for a PWR prior --

MR. ROSA: At the end of every licensing review, we make a site visit and look at all of the electrical systems, DC systems included. That is done routinely. I have done ten or twelve of them myself. And I believe every one of my reviewers has done at least three or four.

MR. RAY: Have you concluded your presentation?

MR. FITZPATRICK: Yes.

MR. RAY: Are there any other questions of Mr. Fitzpatrick?

(No response.)

MR. RAY: Okay, then, we will take a ten-minute break and then go on with Item 3 on the program, discussion of NUREG-0660.

(Brief recess.)

MR. RAY: We will now hear a presentation or discussion of NUREG-0660, probabilistic safety analysis of DC power supply requirements at nuclear power plants, by Mr. Pat Baranowsky of the staff.

MR. BARANOWSKY: Can you hear me?

(Slide)

Actually, we have two other speakers in addition to myself scheduled to talk on this particular item. The report of probabilistic safety analysis of DC power supply requirements at nuclear power plants was done as part of Task Action Plan A-30. I will be discussing some of our review aspects of that report and conclusions and the more technical discussion will come from Mr. Fedele, who will discuss some of the qualitative aspects of our evaluation regarding LER reviews and FMEA analyses, and Mr. Kolaczkowski, from Sandia, who will be discussing the accident sequence analyses and fault tree qualifications for our reliability parts of the study.

(Slide)

I imagine most people are familiar with what the issue is in Generic Task A-30. Its title is "Adequacy of Safety-related DC Power Supplies," and it deals with the adequacy of reliability of DC power supplies required primarily for shutdown cooling nuclear power plants.

And this particular issue involves considerations beyond the single-failure criterion. It involves, in fact, multiple or common-cause failures of DC power supplies and other systems related to the functions of shutdown cooling.

(Slide)

I just thought I would put together a chronology of what has happened, to some extent, since this issue was originally raised in 1977. A NUREG report was published shortly thereafter in which the staff concluded that pending a more detailed investigation, the current design requirements for DC power supplies at nuclear power plants were adequate.

However a task action plan was developed to confirm the particular assessment or provide evaluations which would confirm that assessment if such was the case. That is Task Action Plan A-30, which was originally developed in August of '77 and transferred to the probabilistic analysis staff of the Office of Research in

July of 1978.

A few things happened since the particular transfer; namely, items that affect how people do business in terms of performing probabilistic risk assessments. In particular, we had the risk assessment review group of WASH-1400 publish its report, and the Commission issue a policy statement on the use of risk assessment in licensing actions. And I wanted to point those two items out, since they influenced the scope and length of the program that was underway and continued after that.

In fact, in March of 1979 the Task Action Plan was revised to reflect some of the Commission policy requirements and findings of the Lewis Committee. And another significant incident happened in 1979, in March, and that, of course, was the Three Mile Island accident which brought us more into consideration of additional accident sequences that could be related to the requirements for DC power supplies and reliable DC power supplies.

In March of 1980 a rough draft of the report was completed, and comments were sought by the NRC staff and members of Evaluation Associates and Sandia. And in November 1980 the final draft report, which was provided to the ACRS, was written.

(Slide)

In its simplest terms, the purpose of the study that was performed and documented in the report was to assess the adequacy of DC power supply to some requirements and, if necessary, provide recommendations to improve DC power supply reliability.

(Slide)

In that effort, of course, we had an overall approach which, to some extent, defines the limits of the work and our philosophy on how to perform the assessment. And since the issue was related to the multiple-failure concern, it was decided that event and fault tree techniques should be used, at least in part, to analyze the problem. And in order to provide a generic analysis which would cover essentially all plants, a DC power system or supply design was analyzed, which we felt enveloped the minimum requirements which plants would have in operation today. And, of course, members of the Power Systems Branch have indicated that plants either have design capability beyond that and especially those currently receiving operating licenses or under construction.

In order to bring the concern of DC power supply reliability into the reactor safety area, we assumed or performed analyses which assumed that DC power was required to operate systems to safely cool the reactor. If DC power was the initiating event, it was also required to operate systems to bring the reactor to a safely cooled condition.

And in this case, we tried to maximize the dependence of the shutdown cooling systems on DC power supp'ies. And the way we did it was to take our minimum system and ..it the shutdown cooling divisions evenly between both divisions.

In an effort to update some of the work that was done on the reactor safety study and reported in NUREG-0305, we reviewed and tried to conservatively interpret operating experiences over a several-year period which were relevant to DC power supply reliability. And that was used to essentially generate the failure rates and failure probabilities used in the study.

Variations in D. ,ower design and operation were analyzed to see what kind of improvements could be obtained over the minimum system analyzed, recognizing that plants in fact may have better DC power supply designs than analyzed for the minimum system and recognizing that there may be a need at the end of the program to recommend some improvements. It's nice to know what the value of various improvements might be, relatively speaking.

In order to determine where we might draw the line in terms of making recommendations, the DC power failure contribution to the loss of shutdown coolant and possible core damage which could follow was compared with the likelihood of shutdown coolant failures due to other system or component failures in addition to DC power supplies.

We did this for the minimum system, primarily, and then updated the analysis for several improved versions of the minimum DC power supply design.

(Slide)

At least on these analyses as just described in our approach to the problem, several conclusions were developed. First of all, use of just the minimum DC power system could represent a significant contributor to the loss of shutdown coolant at a nuclear power plant.

This was primarily found to be due to common-cause failures, which we broke down into two particular types, the first being a case in which a loss of AC power to the chargers which might be typified by a loss of off-site power or preferred power, which they are normally operating on, would render them inoperable, followed by both batteries being unavailable due to either deterioration that was undetected in the batteries or buss connection problems and so forth.

The second type of common-cause failure related to operational aspects of the system, either uses of the system resulting in both divisions being incapacitated at the same time or test procedures being inadequate and followed improperly by technicians and operators such that in given circumstances again both divisions could be either deenergized or degraded to the point where they could not perform their function but they would be required to, as part of our analyses of the various improvements and so forth to DC power.

We found you could enhance the DC power supply reliability over what was analyzed for the minimum system by improving therefore maintenance and surveillance and procedural improvements along these lines, as well as eliminating aspects of design which could compromise divisional interdependence rather in your connections, such as a buss tie breaker, for instance.

In providing that the DC power supply is appropriately operated with these considerations, we felt that the failure of DC power in a nuclear power plant therefore could represent a small contribution to shutdown cooling unreliabilty and the possibility of coremelt.

(Slide)

MR. EBERSOLE: May I ask a question at this point? If I turn to page 6-6 of your report, I am going to read the second paragraph: "The total probability per reactor-year of accident sequences leading to loss of shutdown cooling and possible core damage is slightly less than 4 x 10-4 for each study." The long and short of this is the worse you make the plant look in a general context, then the better the DC system will look as a noncontributor.

MR. BARANOWSKY: That's true.

MR. EBERSOLE: Here you have run down to frequency presumed to be coremelt. Which meant for 200 plants to one chance in ten per year that we will have a coremelt. That's a good deal higher than WASH-1400.

MR. BARANOWSKY: It sure is.

MR. EBERSOLE: Why did you do that unless you were seeking to show that the battery system was in fact relatively better than it really is?

MR. BARANOWSKY: Actually, the big change there, as I recall, had to do with the fact that in WASH-1400 the DC power contribution to coremelt was insignificant. It was not really noticeable. Whereas now what we try to do is to make the DC power contribution as large as possible unless there is a bound to what it could possibly be. And if you do that, you will find that DC is the main contributor to that, 4 x 10-4 probability. And that is part of the reason why it is larger.

There are a few other items that we updated in terms of data from WASH-1400 to take into account more current knowledge of either how systems operate or their failure rates which resulted in slightly higher accident probability predictions.

MR. EBERSOLE: Well, you think in 200 plants, which is about what we have, if we build the ones that are on paper --

MR. BARANOWSKY: If we had all plants like this --

MR. EBERSOLE: They're not all like this, thank Heaven, because of the prudence of the vendors and AEs and utilities, and not the NRC people. You don't think that this number is by any means an acceptable number of failure, one in 200 plants per year?

MR. BARANOWSKY: I would think that over a long period of time, there is bound to be a continual improvement in safety, because I am sure that the objective of the NRC -- and I am not trying to state policy that I don't know that much about -- but I think the objective of the NRC right now is to assure that we don't have major core damage accidents throughout the life of various nuclear power plants. And in that respect, one might accept a slightly less desirable design in one plant which met, of course, minimum requirements, knowing that many others had better design. Thus, the average of all plants is considerably better than the most pessimistic analysis.

And I think that for the most part this is a pessimistic analysis. You might find outliers here and there, and I think LERs indicate, not just on DC power but on other things, you are going to have outliers. And so we need to really keep our eyes on LERs to find outliers that are not obvious just by doing paper studies.

On the other hand, we did take the LERs that we had available, and we tried to use those as precursors in many instances to anticipate what possibly might be ways in which we could fail the pipe system, for instance. But we didn't really find total loss of DC power in any plant.

So we are estimating probability based on prior knowledge of precursors that occurred up to a certain date.

MR. EDISON: Could I inject something here a moment? Jesse's question is really germane to what is an acceptable level of reliability for a probability for coremelt, and it is worth knowing that the ACRS has gone on record as recommending that we investigate quantitative goals and that there is an effort elsewhere in NRC to try to set a quantitative or qualitative goal, at least identify how safe is safe-enough criteria for power plants.

We did not do that in this study. And what this number does reflect is not a typical reactor. It is a reactor that, as Pat has described, has a minimum DC power system. And I think you would have to say all the plants -- probably all the operating plants -- are better than this reactor and would have a lower coremelt probability than this, whether this number is the cutoff, better or worse. We are not prepared to say that.

MR. EPLER: I have a question. I note that you have given some comments to the best tie-breaker which impairs the independence of the two channels. I think this is a fairly important consideration. I think this is an important consideration in the design of the systems.

I think just as equally an important consideration that I don't see, and that is the imposition of parasitic loads on a DC system, which repeatedly causes a failure to discharge and causes the plant to scram and then causes the need for the system. I didn't see you give any prominence to that factor, which I think is of at least equal importance.

MR. BARANOWSKY: I guess I can address that. First of all, buss tie-breaker, the main reason for having that so prominently displayed -- in fact, is our number one recommendation -- is that it appears to be the principal place in which you would violate, at least on a physical basis, the independence of a system which is designed just to single-failure criterion, essentially.

The parasitic load problem would be less of a concern if we had divisional independence. But we actually did not neglect that particular item, in that we are requesting that operational matters related to the use of parasitic loads and the nonremoval of them be included in the procedures that will be finally adopted for operation of a system which just has two batteries.

So we are not saying, "Don't worry about parasitic loads." We are saying, "Make sure you clean up your act in terms of the things that can cause single busses or single divisions of DC power to be lost, including operational aspects which could result in parasitic loads in the DC power supplies and proper test and maintenance procedures are not rigorous enough consideration to the human factors involved." And these conclusions are based as much on just a look at the LERs which shows that the DC power supply unreliability for one division typically is a function of those factors.

So it may appear in this brief presentation that we are neglecting a particular item, but if you look in the report, I think you will also notice that the first LER that appears is an incident that occurred at Robinson, at which there was a parasitic load left on a DC buss, causing some problems. And it surprises me that people don't learn from LERs and make corrections in their procedures such that these things have a lower likelihood of happening.

So we are saying, I think, that should be added into considerations of how the systems operated may be in tech specs. These are principles. I am really leaving the conversion of principles to actual licensing requirements to the Power Systems Branch, so I don't think we are neglecting that particular item.

MR. RAY: Dr. Bickel has a question.

MR. BICKEL: I reviewed the report, and I thought there were some good things in it. I mean the idea of trying to find out just how sensitive the ESF systems were to loss of DC power. I think that is a needed thing to be done.

The area I think that concerned me about the thing we were just kind of talking about lightly was there are some very specific quotes I wanted to read. One of them: "It was found that the DC power-related accident sequences contributed about 50 percent of the total core damage probability for the accident sequences studied. It was also found that the contribution to core damage probability could be reduced to approximately 1 percent by implementation of the design and procedural requirements recommended below."

One of the things that I am a little concerned about when I say this is that somebody could take this report and say, "The DC power system is where all the problems are in the ESF systems, and if we take all our efforts, all our money, and all our regulatory programs and direct them towards the reliability of the DC systems, we can cut the failure rate of the EFS, and therefore, core damage, you can cut it from half of the total down to 1 percent."

It leads me to believe -- and maybe I am incorrect because I don't understand the real thrust of this statement -- it kind of leads me to believe that somebody could think the same way I did and we could be putting too much into the area of DC power systems. Could you comment on that?

MR. BARANOWSKY: Of course, you can only say I want to read the words on paper and that's the reason for a meeting like this. I would hope that wouldn't be the interpretation that people would have of that particular statement.

MR. BICKEL: I know. We would hope -- but I am trying to remember was it Zion and Indian Point where they did some other things, like if it took in WASH-1400 it was a quick paper study, but the comment that Zion and Indian Point are 40 percent of the total risk of nuclear power or something, it must be a hundred different places, by very prominent members within the Commission, the commissioners, you know, Harold Denton and everybody. And I think there is the same type of potential really that somebody is going to start parroting that type of a quote, "So we want to really make the EFS systems good; all we've got to do is work on the DC systems."

I just don't believe we have emphasized it by basically taking a crumbling design DC system. And, of course, it would come out looking like it's a big contributor. But I wonder where we go from here.

MR. BARANOWSKY: That's one of the reasons why we tried to show some probabilities of other accident sequences, and we also said this wasn't necessarily a complete study for all other accident sequences. You don't see large LOCA, you don't see ATWS in there, you don't see fire and tornado-type issues in there. If people take quotes out of reports and use them improperly, that's a major problem that occurs all over.

What we tried to do here was give you a rather thick document, lay that on the table, and let you take pick apart what you see. Compared with what I have seen by other people, which is a five-page introduction and 30 pages of results, which nobody knows how they got them. I just don't know what to say about that. If people are going to use the report without looking at the whole report, that's just using it improperly. If you don't like the way it's written, we will try and change a few items.

MR. EDISON: Could I add an interjection here, Pat? The one thing that has to be kept in mind about a quoted number, such as a "50-percent contribution to coremelt probability," is that we are not talking here about a typical reactor design configuration, we are talking about a reactor with a -- I wouldn't say "hokey" -- but a conservative, a minimum DC power system.

That kind of a percentage contribution does not exist in the average here across the spectrum of reactors in our operating plants today or in those that are being licensed, but it does occur in this bounding minimum plant that we chose to make sure that we had covered the spectrum of operating reactors.

The second point that I wish to make is we are dealing only with shutdown cooling systems, not all the engineered safeguard features. And so it doesn't apply to all the EFSs, obviously.

MR. RAY: I would like to pursue a question relative to your comment, Mr. Edison. Can I assume that your recommended improvements are typical of existing plant installations?

MR. EDISON: I am not sure. You mean do we recommend them to be --

MR. RAY: No. In developing your recommendations, the improvements that you would suggest to go from 50 percent to 1 percent contribution, you were guided, I would presume, by typical installations that exist today in a system in the industry?

MR. EDISON: To some extent.

MR. RAY: To what extent? That is the thi g I would like to know.

MR. EDISON: To what extent do the improvements that we considered the range of variations that we looked at, to what extent are they reflected in today's industry? Obviously, in the latest plants, most of these are in -- well, I shouldn't say "most" -- there are no buss tie-breakers being licensed any longer. All right.

So in the plants being licensed today, and in fact for some time now, there have been no buss tie-breakers licensed. There are a few plants, a handful of plants, that had been licensed at a much earlier stage. In terms of maintenance improvements or surveillance or procedures for dealing with testing and so forth, we were recommending those across the board. We think improvements can be made across the board in today's plants in those areas.

So some of these recommendations are above and beyond the current state of practice. And so we did not really dream those up -- I guess you could say we dreamed them up ourselves. We didn't really take this from the plant designs that exist, but we did lay out a fault trip and do a failure modes-and-effects analysis to give us an idea of where we might make improvements.

And, of course, those failure modes-and-effects analysis and fault trees were based on what we know of plant configurations.

MR. RAY: Are you in a position where you can gauge the contribution -- the 50-percent contribution toward core cooling and the 1 percent that is representative of the average plant operated today? Where between those limits do you think the average plant is?

MR. EDISON: I guess -- the average plant?

MR. RAY: Something representing the average of today's industry.

MR. EDISON: I would say some large percentage of the plants, 80, 90, something like that. While they don't have buss tie-breakers, they do have dedicated switchyard batteries. There are going to have to be some improvements made in the way maintenance is done and the testing procedures and surveillance. And we have recommendations -- there will be improvements made at all the plants. They are recommending improvements that should be made in all the plants.

MR. RAY: Yes, I realize that. But you haven't answered my question, and maybe it's because you can't. If you were to assign a contribution to core cooling failure that would be somewhere within the range of 50 percent, which is the minimum, and 1 percent, which is your recommended level, if you will. Where do you think the average plant today would fall in that range?

MR. BARANOWSKY: Let me answer that, because I have looked at this a little more than Gordan. Based on the kinds of analyses that we did and looking at some of the survey data available to us and talking to Faust Rosa about what's out in the field and so forth, I would say on the average plants would be close to ten times better than this minimum system in terms of unreliability, which would mean they would be closer to the 10 percent or 5 percent contribution area on the average.

MR. RAY: Better than the 50 percent?

MR. BARANOWSKY: Yes. But as we all know, there is the occasional outlier, and this study was done to catch the DC power supply reliability outliers, in a sense, in that we are evaluating the minimum to design requirements. So it is really hard for us to judge what the plant average is.

I can see just by looking at them it's not easy to find plants or ways in which the reliability of the DC power system could be much worse than this, excluding perhaps statistical variations in data.

MR. RAY: But impressionwise, you think a characteristic level would be 5 to 10 percent contribution rather than the 50?

MR. BARANOWSKY: That's my impression.

MR. EDISON: Absolutely. I don't believe there are any plants out there with 50 or 40 percent.

MR. RAY: I think that comes through fairly clearly in your report. But I wondered what was representative of the state of the industry today?

MR. EDISON: When you talk about averages, they're hard to talk about what an average plant is, because if you're going to talk about an average of some spectrum of plants, we have to sort of know what that curve looks like.

It could be a strange curve. There may be a handful of plants which are on one extreme and 95 percent of the plants are pretty good -- are very good.

MR. RAY: I recognize your point. But in recognition of Dr. Bickel's point and how little one will recall, if you will, or preserve in one's mind by way of judgment criteria after reading such a report, the prevailing impression could very well be, in spite of all your answers to the contrary, that 50 percent represents today's state of the art and that the industry is in a hell of a shape in this area.

MR. EDISON: We have hassled over that back and forth for many weeks, that that misconception might come across. And I want to emphasize that what we have looked at here is the bounding plant that is not an operating plant, it is not a typical plant, it's a bounding on the lower side. And so this 50 percent is not typical, does not apply to any operating plant.

MR. ROSA: Mr. Chairman, I would like to make a comment on that, too. I have been involved in discussions with Pat and Gordon on the same subject. And in my opinion, I would set the average contribution of the average plant today at about 5 percent or less.

This opinion is based on considering the recommendations of these analyses and what improvements can be obtained by these recommendations and what I perceive to be the average system at any operating reactors.

As Gordon mentioned, I think almost all plants have separate switchyard batteries. Most plants have a nonsafety battery dedicated to nonsafety loads. I would say the majority of plants have as many batteries as instrumentation channels in their safeguards actuation system.

For instance, a two-out-of-four system would have four batteries, one for each group -- one for each division of instrumentation channel. So you see, in addition to that, there are other conservatisms that perhaps haven't been mentioned, like the scenario we are concerned with involves a demand to shut the plant down safely. Occasionally, you get an inadvertent safety injection actuation; however -- or demands to shut the plant down safely. The demand on the batteries is on the order of 50 or 60 percent of that for a LOCA, and the batteries are designed to handle LOCA loads. So there is a big conservatism there.

In addition to that, I noted conservatisms -- there are conservatisms in the surveillance and monitoring requirements on most of the plants that are not even considered in this analysis. So I would put that figure at 5 percent or less.

MR. EBERSOLE: Mr. Rosa, I would like to ask you the following question. About 12 years ago we were looking at BWRs, and it was --

(Laughter.)

-- and, as we know, we're doing something better now. And I think the general practice is before you look at any system to determine what it should be, you look at the consequences of its failure. And we looked at the consequences of BWR failures as a rather horrible thing to contemplate.

Has there, in fact, been one occasion where there has been a hypothesis that there is a totality of DC power failure at any plant and an analysis made of the consequences of that event? This is analogous to the BWR ATWS problem. If you can show me such an analysis, I would be greatly pleased.

MR. ROSA: No, I don't know that any such analysis exists. I know this analysis didn't go that far.

MR. EBERSOLE: Well, it's just like the BWR ATWS problem: You don't know what you're dealing with until you know the consequence. There are several references in here to long periods of time, upwards to an hour or so, when one has recovered if you've lost the system.

I think when the peculiarities of the DC power system if the plant goes into a locked-up state with equipment performing in various uncoordinated modes unprotected and the protective aspects because they have no breaker trips and it may well be that a second DC power failure, if you lumped into the consequence, there's no hope for recovery, because your equipment is now permanently damaged.

I am just saying that may be. I do not know, because I certainly have not done that analysis. I know it has not been done. I go back to my original premise: Before you analyze any system, you must know what happens when it fails, and we haven't done that.

MR. ROSA: You are sort of postulating an open-ended --

MR. EBERSOLE: I am making something credible that you call "incredible."

MR. ROSA: I don't think you can do that, Jess, frankly.

MR. EBERSOLE: I don't think you want to look at that.

MR. ROSA: Well, take this -- I start out with, well, just like the new President --

(Laughter.)

-- this analysis postulates success, given a DC power system failure, of the ability to reinstate core cooling before core damage occurs? And it is based on a time interval given by our core performance branch, I believe, of about one hour as the time required. Now, that's as far as we go in consequences.

MR. EBERSOLE: I understand. But let me postulate, and you can contradict me. But five seconds after DC power failure, the equipment is in such a state of damage that there is no hope of recovery after that, short of rebuilding most of the electrical apparatus.

MR. ROSA: Well, Jess, I personally cannot think of how that could occur.

MR. EBERSOLE: Well, you know, some systems are going to continue on AC, on uncontrolled and unprotected. There is no guarantee you will have trips, as well as guarantee that you will have closure, because you have no control, you have no instrumentation, you don't know where you are, and certainly you are completely shut out. And time now is an interesting parameter of an inconclusive nature.

MR. BARANOWSKY: Faust, let me address that a little bit, please. That might come up in one of the later discussions, but I will address it now.

We recognized -- in fact, we have talked to Jesse Ebersole and know something about this concern. And part of our way of treating it was to say, "If you lost all DC power, the sequence of events that would follow that are largely unknown. And they are probably plant-specific, too."

Therefore, in either the types of ways or manners in which we found that you could lose the two DC power divisions, we assumed that recovery was not possible in this report. The only place that we put recovery in was in cases in which there was like a loss of off-site power and you could recover off-site power excluding both batteries were found to be unavailable.

So, in other words, if I lost off-site power and two diesel generators failed, which would be your station blackout situation, we assume that the plant could go for an hour, an hour and a half, depending on the type of plant it is, in which case we could then recover AC power whether by diesel or by the off-site power supply. If an off-site power sequence involved a loss of all DC power, we never considered recovery of DC power supplies. That was it.

MR. EBERSOLE: Well, do you consider that after DC power failure, that equipment is, in effect, damaged and that you are locked out from a later recovery?

MR. BARANOWSKY: I wouldn't say we specifically included it. But by our assumption that you could not recover and by our assumption that each accident sequence, the failure led to core damage, and this one led to core damage, we inherently included it without getting into the specifics of the consequences.

We could have analyzed a plant, and then we could have had one plant analyzed. It appears that you can recover functions if you lose DC power supply, but it requires some manual actions. But there have been several instances in which one DC power division or one DC power panel has had power interrupted to it, and shortly thereafter the power was brought back by the person typically who interrupted it, except in a few cases like in Robinson, where they had actually degraded the batteries significantly. The problem there, of course, was that they ruined their turbine.

MR. EBERSOLE: Yes. That's a different case. Thank you.

MR. LIPINSKI: Mr. Chairman, correct me if I am wrong, but I believe there is a symbiotic relationship between the diesels and the batteries. The diesels have starters to start on, and I believe the requirement is there be sufficient capacity for six tries. If the pressure in the tank drops down and you still do not have AC power, there is a compressor driven from the station battery to try to restore the air to the compressed air tank and build the pressure back up again. So that the effort to start the diesel puts an additional strain on the station battery to get that tank back up again. And if you still can't start and that particular battery continues to drain down, but to those battery controls, then go back to that same diesel that is trying to start, because those are required, the battery power for controlling the electrical --

MR. BARANOWSKY: I don't know that there is a switching involved there.

MR. LIPINSKI: We still need the DC from the station battery for electrical control.

MR. BARANOWSKY: Yes, but I don't think that operating a compressor precludes the battery from providing power to other components, including what is necessary to start the diesel.

MR. LIPINSKI: Let me ask the following question: What is the current requirement for the operation of that compressor?

MR. ROSA: May I answer that? As of right now, I don't know of any design out there that has a DC motor driving a compressor to supply air for diesel generator starts.

MR. EBERSOLE: Look at TMI-1.

MR. ROSA: Is that the compressor that normally is used to automatically recharge the tanks, or is it a compressor that is manually turned on if the need ever arises?

MR. LIPINSKI: As I recall, it is an automatic pressure control. When the pressure drops below the set limit, the compressor turns on to recharge the tank, and it comes out the station battery.

MR. ROSA: I am not familiar with that design, then. I would be interested to know what horsepower that motor might be. Do you recall?

MR. LIPINSKI: There is also gasoline combustion engine standing right next to it, such that if the battery is dead, then you can start that engine. And it has some little battery starter on that engine as a standby source. But the fact that the diesel can fail to start -- now, the next question I have, really, is: What is the statistics in terms of the diesel failing to start on six tries? Has this ever occurred?

MR. ROSA: It's generally recognized in the industry that if you fail to start within three tries, you can forget it. There is something that went wrong with the engine that cannot be fixed. We require six starts as the margin, really.

MR. LIPINSKI: Okay. Well, that only guarantees that the battery associated with that diesel is on its way down for the entire period.

MR. ROSA: Well, as I say, I don't know what size that motor is. And if that occurs, it occurs only on one diesel generator. I wouldn't expect something to happen on both. And therefore, you know, you restore one diesel, which would then supply any charging air requirements through the battery charger.

MR. BARANOWSKY: Could I also add one point here? In that particular concern is the kind of thing that we will be looking at in the station blackout program; that is to say, what are the DC power supply capacity-type requirements given that you don't have a safe power to the plant? It wasn't really studied as part of DC power supply reliability. We said, "Do you have DC power at the outset of the event?" And if it's a blackout type of event, we couldn't expand this program into another issue without, you know, extensive additional resources, and we wouldn't know where to draw the line, so we drew it there.

MR. LIPINSKI: But it's not one of your design requirements that the station battery be used to drive the compressor to restore the air tank pressure?

MR. ROSA: We don't even address that issue.

MR. LIPINSKI: Because I didn't see it on any of these diagrams, the fact that there are these paths that are not electrical paths, but they are energy paths.

MR. EBERSOLE: In general, a failure is ordinarily considered to be a failure of a given function not to work. It has heretofore not been considered in excess of that failure -- it is a failure, like too high pressure, whatever.

I think there are sufficient people in here to contemplate this question, and maybe you can answer this. Is there anyone who can tell me if I postulate an instantaneous failure of the totality of the DC plant, which is the second failure, the first having failed and cascaded the second, how does the AC power system work, not considering the diesels but considering the off-site incoming power, the turbine generating power, not the diesels?

Do we have an AC system which is now running rampant, uncontrolled, with main feedwater continued at its prior set point to overfill steam generators and excessive water which is under some sort of control and being controlled and now unable to respond to the present position that it's in?

In short, do we get an uncontrolled flow of AC power which will lead to complex situations such as overfill?

MR. ROSA: That's a possibility in a system that just has two batteries and uses it to provide all the load safety or non-safety.

MR. EBERSOLE: I postulated the DC failures.

MR. ROSA: There is no avoiding it, unless of course the DC power supply to the non-safety loads, for instance, the high -- main feedwater flow affected the control section of the main feedwater flow, the control valve was closed or something like that.

MR. EBERSOLE: I only used this to illustrate the fact that we don't really know.

MR. ROSA: We don't really know, and you can also state that we don't know an infinite number of other things, and where do we stop looking at this infinity of sequence.

MR. EBERSOLE: We stop when we believe it's incredible that a failure occurs.

MR. ROSA: Well, then, Jess, I will have to say in my opinion we have reached that point.

(Laughter.)

MR. EBERSOLE: With two trains of DC.

MR. ROSA: Not necessarily.

(Laughter.)

MR. EBERSOLE: We're somewhere in the middle of something.

MR. BARANOWSKY: I don't think we're saying two trains makes anything incredible. In fact, being involved in probabilistic analysis I don't know what "incredible" means. All we are saying is that with two trains of DC power, with appropriate care in the operations of those systems in assuring that they have divisional independence, that the likelihood of their failure occurring is not so large that it is as dominant as we have analyzed in this; in fact, significantly smaller and comparable or less than many other types of failures which could get you into a serious condition with the reactor.

I don't think anyone should construe that to mean that we feel that you can have a failure of DC power. That is not what we are saying. We agree with your point that we really don't know exactly what would happen if we lost all DC power, and I don't find that to be acceptable, and I don't think that is the conclusion in this report.

We may wish to debate how safe is safe enough and hence the level of reliability which we have identified in our recommendations; but I think we are really saying the same thing except perhaps for the level of acceptable reliability.

MR. DAVIS: Excuse me. Do you have time for a couple more?

MR. BARANOWSKY: Sure.

MR. DAVIS: Someone brought up the problem of taking stuff out of context, and that gives me an opportunity to ask my questions.

(Laughter.)

The trouble I had I guess with the report, and I didn't have time to study it in detail, so it might be partly my own problem, the report comes to a conclusion about the probability of core melt or core damage from electrical power problems. It gives a quantitative number that is quite high; in fact, it alarmed me some because it's higher than the total from all accidents out of WASH-1400. And then it says because of the conservative nature, this assessment agrees with NUREG-0305, and 0305 says it's no problem; in fact, the probability of core melt from power failure is essentially what was said in WASH-1400, and the numbers are considerably lower than what 0666 says, and I could not make the transition. I couldn't come to that conclusion from the information you gave, because there wasn't any analysis of a typical system. In other words, the assessment was not realistic because it was much more conservative than any system.

But the obvious question, it seemed to me, is where do the actual systems sit, and how can you draw the conclusion that it's not a problem? And maybe I missed something, but I really couldn't make that connection.

MR. EDISON: I think I corrected this statement on page I-3 about confirming. NUREG-0305 reads as follows: "The word 'report' here generally confirms the earlier assessment reported in NUREG-0305."

Now, the earlier assessment was a preliminary assessment that was done in a much shorter period of time with fewer resources, and they did quote smaller probability numbers. And what we are saying here when we say we generally confirm that assessment is that I think we confirm that from a perspective of all the accident scenarios that we can think of -- small LOCAs, transients, whatever -- that the DC power contribution is not the dominant contribution in today's reactors.

Generally we do confirm that, but this particular bounding configuration is dominant, and of course the earlier assessment did not look at this bounding kind of thing. They tried to look at a typical system.

Now, if we go into some of the improvements in sensitivity studies, we can try to reproduce some kind of typical system and come up with another number. But our intent -- what we want to get across, what we want to say in that particular paragraph is that we do confirm their judgment that this is not the dominant sequence or contribution to go running out and putting our resources on.

We have not agreed with them in the sense that we say there is nothing more to be done. We have made recommendations for some changes, so we have gone further than that report did; and we are recommending some changes be made, whereas that earlier assessment did not. Furthermore, we have additional data. We have improvement in our systems analyses and our failure data. We have some 250 more reactor years of experience now which about doubles the operational data base we had at that time, so we have improved the analyses.

But to summarize our intent in stating that we generally confirm that earlier assessment, it is in perspective to other accident scenarios.

MR. BICKEL: Mr. Chairman, I still kind of -- I think the question -- I think it would answer a couple of our questions -- maybe I can try and phrase it this way.

We all have some kind of a feeling for what DC power does to making accidents good or bad. If I were to give somebody a million dollars and say I want you to improve reactor safety and the ability to cool a core, would you take the recommendations you had that came out of NUREG-0666 and say these are the chief things we should do to assure that we can cool the core or what else, because otherwise you have no perspective as to how important this thing really is.

I think that is the real thing you want to get out of a study like this, isn't it?

MR. BARANOWSKY: Let me just take a little bit of a crack at that. The problem is you're talking about taking a generic assessment and asking me to go out to all the plants with a limited resource and saying what I do on plant A I might not do on plant B, because there has been a lot of flexibility in how people have been able to design their power systems and their engineered safety features.

And to say across the board I would spend a million dollars on one item, especially when there are other things identified even in this report that can be contributors to reactor safety, that would be a little bit hard to say. But one way to go about spending a million dollars or any amount of money effectively is to develop an improvement which cuts across more than one accident concern line of thought, you might say; and that way you may be more cost effective in improving the plant.

And I think we have some work going on in the NRC with regard to improved safety that talks about doing these kinds of things. Meanwhile, we have issues of a more specific nature, DC power, AC power, and what not, and we address them as we come along.

I don't think that the recommendations that are made in this report are very substantial in terms of outlay as compared to what I have seen done after the Three Mile

Island accident, for instance. I think these are minimal, and I wouldn't want to compare these recommendations with the building of special centers and so forth in terms of outlay of resources.

MR. EDISON: We've already studied that less than five percent in the operating plants. If you want to proportion the money in that kind of a linear fashion, you would say less than $50,000.

I'm not sure you would proportion money that way. I think what you would do is take that dominant contributor and maybe go at that 100 percent. It depends on how you wish to attack it.

But I think that impression has to get across that we do not consider this a dominating contributor in the operating plants, and we've not put our resources on it. I can tick off a few contributors that I think are much more dominant and where the Commission is working on it much more heavily. There are a number of unresolved safety issues -- not just A-30; there must be 30 or 40 of them -- to get resources and then work on. There are plant-specific things that come up periodically.

But the purpose of our report was not to come up with a research budget on how to allocate our resources.

MR. ROSA: I would like to interject something here, too. From a practical standpoint, if I came across a plant with this minimum design and I had this million dollars that you're giving me, I would use it to install another battery in the plant to take care of non-safety lights, to install another battery in the switchyard for switchyard control power, and to upgrade the maintenance and test procedures associated with DC power systems to make sure that they meet the recommendation there and also meet the other one which is remove the buss tie capability.

MR. RAY: Okay, Mr. Baranowsky.

MR. BARANOWSKY: Well, I guess we've discussed the recommendations.

(Laughter.)

I think you pretty well know our conclusions. I believe the next step would be to ask Mr. Fedele to come up here and talk about some of the details that went into this work, and then he will be followed by Mr. Kolaczkowski.

MR. RAY: Before we release him were there any other questions of Mr. Baranowsky?

MR. DAVIS: Mr. Chairman, excuse me. I have one quick one.

I noticed that there was no mention in the report of the influence of the power failure accident sequences on the containment safeguards. As we all know from WASH-1400, not all core melts are equal. Some pose almost no risk while others can be substantial.

And I was curious as to why you did not consider whether or not the containment would be protected by the operation of containment safeguards, and the table in there compares all these sequences on an equal basis, and yet it appeared obvious to me that some of them would definitely result in containment failure; others probably would not.

MR. BARANOWSKY: Well, we didn't include a risk assessment. The next step beyond what we did here in the evaluation, not that I don't think that kind of thing is desirable, but actually the resources were somewhat limited.

And at the time that this particular program was put together, it was directed at DC power reliablity; and we took it a step further into the core melt domain, which is the way the issue was described, and that's the way the program went.

I can tell you that when we do the blackout part that we will be doing not only the probabilistic but the risk part in addition to it. So, yes, we are deficient in that one.

MR. RAY: Okay. Mr. Fedele.

MR. FEDELE: I am going to talk about the failure effects analysis, the LER review, and show you the summary of the fault trees that we developed.

(Slide.)

The first chart is the system, the DC system that we looked at. It's a schematic, a simplified schematic, and shows two busses with the tiebreaker, which is normally open. We have one battery charger and one battery per buss, and then we go to the various loads, typical DC loads.

MR. EBERSOLE: Pardon me. Right at this point I'd like to ask you a question. Did you measure calculations and reliability estimates on a stabilized battery charger that can function adequately without the battery as a stabilizing agent?

MR. FEDELE: Yes.

MR. EBERSOLE: Isn't it a standard specification? It is in some plants, but there are chargers in place which do not function without the stabilizing influence of the battery. Have you factored that into your --

MR. FEDELE: No.

MR. EBERSOLE: Are there any requirements in the reg about this?

MR. ROSA: We presently require that the battery charger be capable of operation without being connected to the battery.

MR. EBERSOLE: How many plants do we have that don't have that?

MR. ROSA: I don't know.

MR. EBERSOLE: Thank you.

MR. BARANOWSKY: Let me add that a portion of the analysis, at least that had to do with common mode failure, considered that the charger may not be able to function if the battery is taken off and it's not tied, for instance, to another division.

MR. EBERSOLE: Thank you.

MR. EDISON: Let me also add, Jesse, that that portion was the dominant portion of the analysis, the common mode failure.

(Slide.)

MR. FEDELE: This next slide shows the typical two division AC and DC system. We have two diesel generators and a battery charger with the battery supplying the safety loads and the switchyard; and this is the system that we used in this particular analysis and configuration.

(Slide.)

The next chart summarizes the shutdown cooling systems that were considered in this study. In the PWR we have the main feedwater, the aux feedwater, the high pressure injection, and the reactor coolant system safety relief valves. In the BWR we have the main feedwater power conversion system, the RCIC, the HPCI, the LPCI, the RCIC, the low pressure and automatic depressurization system, and your service water systems.

MR. EBERSOLE: May I ask a question on the PWR supporting systems such as service water component cooling and the environmental control systems and a host of other things which are part of the shutdown function --

MR. FEDELE: Well, when we considered the DC system in doing this study, all we wanted to do was to look at the actual system itself and how it is affected by loss of DC, not by the support system.

MR. EBERSOLE: Well, the load systems, of course, are affected by DC, too. Well, in any case the view is that you have the --

MR. EDISON: The action of these systems to assess their failure rates and their error base was considered in a sense that when we quantified the failure of these essential cooling systems, the contribution of those systems to the failure of these systems was included.

MR. EBERSOLE: Was included in the context of these first systems you have here, but you didn't do it on the right side. For instance, you have high pressure service water system on the right side. Evidently it was done by a different man.

MR. BARANOWSKY: Well, it's a little bit more directly important, you might say, on the BWR, whereas it is indirectly on the PWR. It's just a question of how to display it.

MR. EBERSOLE: Then I can look at the four items up there and say there is embodied in those four a number of other service systems.

MR. EDISON: Absolutely.

MR. EBERSOLE: Thank you.

(Slide.)

MR. FEDELE: These next two charts illustrate the way we divided the AC and the DC power for the PWR and the BWR. What we did is we maintained the single failure criterion and redundancy, while at the same time apportioning the DC dependencies amongst the different subsystems that were involved in this study. That's the PWR, and the next chart is the BWR.

(Slide)

And that is essentially the same or similar.

(Slide.)

This next chart shows a summary of the results of the failure mode effects analysis. The intention of the failure mode effects analysis was to look at each component in the DC system itself and to postulate failure for the individual components and then propagate the failure modes up through some system effect.

The main components that we looked at were the battery recharger and the battery -- the buss itself and the buss tiebreaker. And one of the reasons for doing this analysis was also to see if there were any common mode failures that would knock out both busses. This would tell us whether one buss would be knocked out, but also by propagating the failure properly, we could tell whether it would knock out both busses due to single component failure.

(Slide.)

During the study we'll do quite a few hundred LERs, and this table summarizes the LERs we reviewed, and they date back from 1969 to roughly June 1979. They include all the LERs that are involved with electrical systems, batteries, cables, relays and what not -- the components that are typically used in a DC power system.

We evaluated these to confirm the failure modes, to find additional failure modes, and also to use the data to generate failure rate for the individual component system.

(Slide.)

Now, this chart essentially summarizes the failure modes that we identified either from the FMEA or the LER review. For the battery charger we found that there were a lot of failures in high output current where the voltage was high or low, erratic performance on the output. Chargers were tripping for various reasons, and there were continuity failures, open circuit, open and short connections either inside or outside the charger.

There were failures where there was either low voltage on the output of the battery or the output of the battery itself, the current was low, the redamaged batteries buckled plates, and also continuity failures. This is your cable failures. The buss tiebreaker did not find any shorts to ground or to the DC return.

Specifically on circuitbreakers themselves, they would apply so that it's really the postulated failure mode that we did in the FMEA itself. There were buss losses due to many reasons -- operational, errors, test and maintenance errors, and there were busses that were degraded due to malfunctions of your charger where the charger itself went out and the battery itself was degraded, and also there were buss voltage degradations which were caused by loss of offsite power or you lost your charger and your battery was not up to snuff to give you the power that you wanted.

(Slide.)

Now, this chart is a simplified fault tree of the DC power system itself. What we have are common mode failures of the DC system and independent failures of the DC system. Both of these lead to loss of the DC system itself. The common mode failures -- the dominant failure mode was loss of AC input to the charger combined with an unavailable battery, batteries that were degraded. Then we had common mode failures with the buss tiebreaker closed where operational errors caused both busses to be degraded and/or test and maintenance errors resulted in de-energizing the busses.

On the other side we have a coincident but independent failure of two busses, and what we show is one buss failure where again we have the test and maintenance errors, but this is errors that cause you to lose one buss, and operational errors again that cause you to lose a buss, and coincident failure of the battery charger and the battery itself. And this is principally the summary of the fault tree for the DC.

(Slide.)

Now, this final chart briefly summarizes the fault tree for shutdown cooling system and how we handled it. We developed a -- we have DC system failures, and AC failures, and shutdown cooling failures, further reasons. What this means is that DC failures or shutdown cooling system failures are failures that are related to DC malfunctions, and then you have AC failures that are related to AC failures. And then on the far right we have failures of the shutdown cooling systems for other reasons of their own.

Are there any more questions?

MR. RAY: No questions for Mr. Fedele?

Mr. Bickel.

MR. BICKEL: Yes, one quick one. You have shown in your -- I think it was one of the first tables you showed, that battery charger trip leads to reactor trip. I assume by that you're saying in a very, very prolonged sense.

MR. FEDELE: It was the first one?

MR. BICKEL: It was up in the front.

MR. FEDELE: Oh, you mean in the FMEA summary.

MR. BICKEL: Yeah. I happened to look at a lot of LERs related to that area, and the usual event is that you get an alarm like say a low voltage alarm. The operator goes over, and he resets the trip, tries to figure out what happened. And I don't think -- I looked at an awful lot of the study I had done, and I don't think I even saw one that actually led to reactor trip.

There may be one or two from other years, but the time scale is a thing that I think -- you have got a bit of time. You are going to get an alarm saying that you're starting to discharge the battery, and it is not being recharged. You get a low voltage alarm, and that's obviously going to send somebody out to try and find out what's wrong, because he's got time to reset the thing.

I can see -- I gather what you're saying is you assume you let it fail and just let it sit there for however long it takes to --

MR. FEDELE: Is this the item you're talking about?

(Slide.)

This is not time based. The system we are looking at actually is alarmed. There are low voltage relays and guard meters and what not. What we are postulating here is that your battery charger -- well, for example, during an equalizing charge there were failures where the equalizing charge went up to 147 volts and damaged the battery, and as a result I looked at that and I said okay, suppose that were to happen, what would be the result? Would we lose the battery and the charger, and of course we'd lose the buss. And it postulates in there that if we lost the buss, we lose -- we will trip the reactor.

MR. BICKEL: Okay. I see your point.

MR. DAVIS: Mr. Chairman, a quick one again.

I don't want to try to resolve this now, but the next to the last fault tree that you presented, the top of it is the DC power system failure. It doesn't seem to agree with the corresponding fault tree on page D-3 of 0666. I had some problems with the tree on page D-3 which I think you have corrected in this one.

I just wanted to point out to you if you're still using this one, I've got some problems with it, but if you're using the new one, I don't have a comment.

MR. FEDELE: Wait a minute. This one --

(Slide.)

I don't know which one you're talking about. No, we corrected that. They'd be in real trouble if that were true.

If that's all the questions, I will turn the presentation over to Mr. Kolaczkowski.

MR. KOLACZKOWSKI: Thank you, Mr. Fedele. Good morning, gentlemen and ladies.

Okay. As was mentioned by Mr. Baranowsky earlier in our presentation, I'm going to discuss the quantification aspects of this study and also highlight again some of the results in the improvement in sensitivity analyses which we performed to give added perspective to those results in this study.

(Slide.)

Okay. The first phase of the quantification analysis involved taking a look now at the primary components in the DC system -- that is, the batteries, the chargers, the busses themselves -- and proceed with the quantification of the failure probabilities of those particular components.

What you see in this vugraph is essentially a summary of that analysis, and because we are interested not only in single buss failures but also the possibility of multiple buss, you can either do common cause or independent events. We needed to quantify also not only the single failure battery rate but also two battery failure rates; again, the chargers which can be affected also by the loss of offsite power and then the single and multiple buss loss due to operational and test and maintenance type errors.

On the right hand column under "Basis," that is there to show essentially what our primary basis was for the failure probability estimates shown on the vu-graph. In most cases you can see that the evaluation came from the LER review where we identified how many failures we saw based on the number of reactors used that were in evidence, based on that review and three rather simple techniques, end up with a quantification for the failure probabilities of the major components of the DC system.

I do want to highlight this one thing with regard to the last thing on there, the multiple DC buss due to operational and test and maintenance in the LER, we did not see any such cases where human errors have caused a degradation of two DC busses in the context of a minimum system, for instance. But we did do a precursor type analysis recognizing that some of the kinds of operational and test and maintenance failure modes that we did which de-energized this thing called buss could, under varying circumstances, for instance, if you did have a buss tiebreaker cause could cause a cascading type effect and take out both busses of a minimum system.

It was through analyses of this type that we were able to estimate the failure probability for that last item.

(Slide.)

MR. LIPINSKI: On that last one where you have the charger failure 2 X 10^{-2}, immediately if it drops off --

MR. KOLACZKOWSKI: Yes. I think that's true, that in most cases I would have to -- I'm not sure again whether we include in the minimum the same requirements, the consideration that you would get; but I think in most cases, yes, you would get an indication that the charger --

MR. LIPINSKI: Because if it's only on battery voltage, then you're waiting for the battery to have been discharged to the minimum voltage acceptable level. In order to indicate a charger failure, there are two ways to do it: one, monitor the charger current directly such that when it drops off it is immediately enunciated; but if you wait until the battery discharges, this occurs later in time until you hit the trigger point for minimum acceptable voltage.

MR. KOLACZKOWSKI: I think those considerations were gathered from the FMEA.

MR. LIPINSKI: So charger failure does not necessarily contribute to single battery failure on the top line on a one-to-one basis.

MR. KOLACZKOWSKI: No, no.

MR. LIPINSKI: Because I can detect charger failures before I get to so-called battery failure.

MR. KOLACZKOWSKI: Yes, absolutely.

(Slide.)

Okay. With failure probabilities of the key components quantified, now if we plug those into essentially the simplified fault tree that Mr. Fedele showed you just moments ago, you then come up with a quantification of the DC system failure probability.

You will note essentially first of all with regard to the common mode, again as Mr. Baranowsky also mentioned in his presentation, we were able to categorize those into basically two types of common mode failures -- the loss of AC input to the chargers, and would most likely occur due to a loss of offsite power to the plant; and then both batteries being unavailable for a variety of reasons.

The system effect would be loss of both busses by common mode, and you see the point estimate probability based on the values on a previous slide.

The second category is the operational and test and maintenance type areas, particularly while the buss tiebreaker would be closed, and you would be doing some maintenance on the minimum system. That by itself would cause loss of both busses directly by that initiating event, and again you see the point of probabilities shown.

We also looked at the loss of both busses due to independent means and the loss of the single buss, and again in this case there are essentially two major categories or types of failures for loss of a single buss, and you see the point as probabilities shown there per reactor year.

(Slide.)

MR. LIPINSKI: What's the difference between line 3 and line 1 on the loss of AC input to chargers?

MR. KOLACZKOWSKI: As far as line 3 is concerned, when we say both batteries fail independently, we mean that due to either an error caused by, for instance, the operating performing incorrect maintenance on both batteries -- in other words, he does it wrong in the first and then does it wrong in the second dish. He would be the common mode link, if you will, whereas in the third line we were talking about truly independent failures that would most likely be due to hardware failures within the battery itself that just happened to concurrently occur.

MR. LIPINSKI: You've got your initiators' loss of AC.

MR. KOLACZKOWSKI: True. That takes out the chargers. And then the point is that both batteries, for instance, could have become degraded due to some mode effect. Again, I've tried to give an example of possibly incorrect maintenance as being the common mode link, or it could just be coincident to independent failures of the remaining two batteries.

Maybe I don't understand your question.

MR. EDISON: The focus here is on loss of buss, and what he's got is what it takes to get there, first the chargers, then the batteries, how you get there.

MR. LIPINSKI: Okay. If I lose my buss, I'm going to get an indication that that buss is lost, and if I don't recover diesels, because this requires total loss of AC, offsite as well as diesel in order to have loss of AC in two chargers, that would be immediately enunciated. There is no charger output, and then if this condition persists, then naturally you lose both batteries.

MR. KOLACZKOWSKI: Okay. You talk about loss of offsite power in the diesels. First of all, we again in our maximizing our dependence on shutdown cooling -- excuse me -- for shutdown cooling on this system, if the loss of offsite power occurred, if the batteries were unavailable at that point, then we said that you would not be able to start your diesel, set the diesel starts, required power from the DC buss.

MR. LIPINSKI: But the battery failure is subsequent according to your column. I have the initiator and then I have the subsequent failure.

MR. KOLACZKOWSKI: I wouldn't put too much emphasis on that. That could be intermediate. The batteries could have been degraded between now and the last time you did test and maintenance. This was not -- we saw cases in the LERs of that being the case, and suddenly when you have LOP, the batteries aren't geared to supply the load to start the diesels.

MR. LIPINSKI: So "subsequently" doesn't mean subsequently. It might have been silent failure of the batteries, and you don't appreciate it until you lose the charges.

Thank you.

(Slide.)

MR. KOLACZKOWSKI: Okay. Another factor we had to be concerned with is what initiating events were we going to look at in the study, and this summarizes which ones we did and mentions also a few that we did not include.

The items that you see above the dotted line are the initiated transients that we did include in this analysis and their approximate frequencies of occurrence. Besides the one that's already been mentioned, that is, DC power failure either of a single or multiple buss being the initiating events, so besides that one these are the other initiating events that we did include.

Below the dotted line you see mentioned, too, the large LOCA and severe reactivity transients, and it was such we did not include it in this analysis. That was primarily using a probabilistic criteria recognizing that they are considerably more infrequent as compared to many of the initiating events up above, and the fact that the initiating events up above would still require you to do to your ultimate shutdown cooling systems.

We used this probabilistic argument to rule out the latter ones down below. Again, they would not add significantly to the overall analysis because of their relative infrequency as compared to the ones up above.

MR. DAVIS: I have a question, Mr. Chairman. What's the basis for your loss of offsite power frequency point two?

MR. KOLACZKOWSKI: We did an LER review and also got some data from another survey which -- I'm not sure, I don't know if it's been published or not.

MR. EDISON: There was a survey taken on the operating plants, and that data has been analyzed. That number -- that's a national average number. Take all the losses, divide by the number of reactor years. It's fairly accurate, we think.

MR. DAVIS: It's the same number in WASH-1400.

MR. KOLACZKOWSKI: The number we used, if you want to get down to some decimal places, was .22, but this number did not come directly from WASH-1400. This is a separate survey.

MR. EDISON: When you mentioned the WASH-1400 relation there, there is a point I wish to make, and that is that after the WASH-1400 study was done, and Mr. Baranowsky mentioned that the risk assessment review group reported, we got a policy statement from the Commission that told us that to use WASH-1400 data verbatim without examining it and being sure there is a sound basis. We sent formal direction of that nature to Sandia for these analyses, and we incorporated it ourselves in these various data that we have used -- the LER reviews, the operational data, etcetera.

They've all been newly examined with agonizing over individual LERs as to whether this is a failure to come up with new data; especially the offsite power data are all new and represent operating plant surveys directly with the plants and their responses.

MR. DAVIS: Okay. The reason I asked the question is the report by Abbott, Bickel and Merriweather seems to argue for frequency of about half of that. Looking at the number of offsite power losses that have occurred over a three-year period covered in that report, and considering the number of reactor years of operation, I get a number about half of that. It probably won't make any big difference.

MR. EDISON: It wouldn't make any big difference, and I wouldn't get concerned that. The frequency range is as high as one at some plants, one lost annually, in some plants very, very small. And depending on how you interpret certain losses, whether it's been a total loss or a partial loss, you can ficker around with that number and get it to run between .1 and .3 or so.

We have done the best data analysis we can to come up with .22 at the current time. But I think we are really talking about a small percent as compared to some of the numbers.

MR. BICKEL: The number you're thinking of is the loss of a single circuit, not a complete loss of offsite, if you take a close look. I said it is more probable that you're going to lose a single circuit, but that doesn't generally lead to reactor trip.

MR. EDISON: I'd like to also comment we're going to pin that number down even a little better in the station, block out generic issue tab A-44.

MR. LIPINSKI: Is loss of offsite power directly reportable then under the LERS or does it come out due to reactor trip and then you have to look for the reason for reactor trip?

MR. KOLACZKOWSKI: I don't think I can answer that question.

MR. EDISON: I think in the past, earlier, some years ago that it was not required to be reported. I'm under the impression now that the plants are reporting it. In fact, I know they have to now. They report it to the incident response center, and it gets logged. But the LER form, it does not require that to be reported.

MR. LIPINSKI: The B&W plants were designed to withstand the turbine trip. That is changed now as a result of TMI-1. But the original design was to ride out a turbine trip by the control system designs.

MR. EDISON: Some of those offsite powers were not reported in LERs, in fact, and so that's why we went back and surveyed the plant, sent them bulletins and requested that information. We gave them a detailed list of the information we needed about offsite power and they are responding. Most of the plants have responded now..

MR. KOLACZKOWSKI: Okay. Another aspect of the analysis involved in identifying the accident sequences that we need to be concerned about --

(Slide.)

-- And I'm going to show the two event trees which were constructed when, one for each plant tied to the PWR and the BWR, and I just wanted to point out a few things with regard to the event trees.

First of all, regarding the construction and the headings across the top, you can see that we broke out separately the DC and AC electrical systems as separate events on the tree. We include, of course, the main feedwater system which would be the normal means by which you would remove decay heat given you had a reactor trip and you need to go to shutdown cooling.

And then given that might fail, then of course you pull in the ultimate shutdown cooling systems which were mentioned already in Mr. Fedele's part of the presentation.

Another feature I want to point out is that we broke out DC power separately and put it right out in front in the event trees for a reason. From both a pictorial point of view and also from an analysis point of view it made it easy to compare those accident sequences, for instance, the ones you see here, which do not contain any contribution from DC power failure. And I've shown strikingly in red -- maybe that's an appropriate color.

MR. EDISON: One day after the hostage release that's an appropriate color.

MR. KOLACZKOWSKI: The same accident sequences but now containing failure of either one or both of the two divisions of the DC power system.

The third thing I want to point out, and it kind of comes back to some of the comments that Mr. Ebersole made earlier during the presentation, you can see that we said the total loss of DC power led directly to core damage. We did not try to analyze the sequence in detail, but we recognized that given a plant with this minimum system, for instance, a number of things could be going on if you lost all DC power. For instance, you would have a loss of much of your vital instrumentation in the control room. The operator would be flying blind to some extent with regard to his plant status.

Again, because of a maximum dependence on DC power for shutdown cooling he probably would not be able to initiate and control his shutdown cooling systems from the control room. And so there were things of this sort that we recognized, and rather than trying to do a detailed analysis of what the scenarios might be, because they could be plant-dependent, we just said the total loss of DC power in the plant would lead directly to core damage.

(Slide.)

Okay. This similarly, if you look at the BWR again, the same sort of features apply. We broke out the electrical systems separately, looked at the power conversion system which would again be the normal means for removing decay heat, and the included the shutdown cooling systems of interest. And again the structure is the same as a PWR, with regards to the sequences that do not contain a DC contribution and those that do.

MR. LIPINSKI: Could you go back to the PWR?

(Slide.)

As to how you select your sequences, as to which you want to indicate first and second is very important, but there seems to be one path, that is loss of AC with a stuck-open PORV leads directly to coremelt, because you assume you did not have your high pressure makeup under those conditions. The loss of AC is a stuck-open PORV and would lead me directly to a coremelt.

The steam turbine is not available, according to your layout there, if I have a break and the energy is going out the break, so that there is no steam turbine.

MR. KOLACZKOWSKI: What we said is that if you have lost RCS integrity for whatever means -- and one example would be that the PORV is stuck open -- there is an additional need for makeup in the plant, and if you can't get AC power back -- in other words, if there is no recovery event, you can't get your

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

makeup system on, and eventually you will go to core damage.

MR. LIPINSKI: All I'm saying is if I wanted to redraw your diagram, I would have one sequence, loss of AC with loss of RCS integrity leading directly to core damage.

MR. KOLACZKOWSKI: You could do that, that's correct.

MR. LIPINSKI: It's the choice of whoever draws the diagram as to the sequence you want to show these.

MR. KOLACZKOWSKI: That's correct.

MR. LIPINSKI: Similarly, on the BWR diagram --

(Slide.)

-- I puzzled over this one a while, because all sequences require residual heat rejection system, and then going to your appendix, it becomes obvious that these pumps are all AC-driven.

So, again, with the sequence of loss on AC, you get led directly to core damage.

MR. KOLACZKOWSKI: Okay, that's true, and you could structure it that way. We structured the tree this way to try to show, first of all, you know, the support system is kind of up at this end, and then as far as the rest of the structure of the tree is drawn almost in a way in a time sequence kind of thing, saying that following the initiating event, again depending on what has happened, you may try to get your high pressure cooling systems on first.

If that doesn't work, or if you are depressurizing

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

because you have a break in the system somewhere, then you are going to go to your low pressure systems, and we show that, but then eventually you do need that residual heat removal.

But you're correct, you could draw the tree a number of ways.

MR. LIPINSKI: You get led to the end result directly, whether you have or have no DC.

MR. EBERSOLE: In regard to that, eventually you mentioned, I think it was something like 27 hours in here some place about a BWR heat-up. Invariably every one of those time extensions up to 27 hours is based on looking at the pins of the fuel -- the core, in other words.

There may very well be some environmental temperatures rising at a much faster rate than that, to the extent that equipment which you will need later will not become available when you can use it like in 27 hours.

I think one of the omissions in the study here is to look at heat-up rates in an environmental context on equipment other than the core.

MR. KOLACZKOWSKI: This does take into account equipment other than the core. The 27-hour sequence that you are referring to, I think we will try to put a little more emphasis on the fact that you may be removing heat from the core, for instance, by your high pressure cooling systems, but you still need residual heat removal, because the heat is just being

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

transferred from the core area to the suppression chamber, and now it's the fact that you really need residual heat removal system to start cooling the suppression chamber and not the core is the reason why if you don't have it, you --

MR. EBERSOLE: Okay. That happens to be the suppression chamber that you are looking at there. I'm saying if I look at systems other than suppression chamber, look at, for instance, the RHR or HPCI rooms, or look at all cooling systems, equipment cooling systems which are locked out by thermal effects long before the suppression pool or the core has got too hot, to the extent that they are nonrecoverable when you could later on use them.

MR. KOLACZKOWSKI: Again, the heat rejection system -- now it's been defined in the report, but that also includes a service water system, the high pressure service water system, and we said you needed all of those to provide, among other things, pump room cooling, or this may be low pressure injection pumps and that type of thing.

So it has been implicitly included.

MR. EDISON: I think Jesse Ebersole has a legitimate point here. In our kinds of analyses we do not investigate system by system, pump by pump, wire by wire, what happens to that equipment. From a high temperature steam that might occur during the accident, for example, we presume that it functions when it is needed, aside from the environmental --

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

in spite of that. It's a weakness.

MR. EBERSOLE: I think in the case of Browns Ferry, the termination of a nonrecoverable time period was something like a few hours due to ambient overheating in one of the rooms some place that led to a lubrication system failure long before the suppression pool was too hot or the core was damaged. And what it did, it damaged and locked out equipment beyond further use, when they could have used it later on.

MR. BARANOWSKY: This was the kind of stuff that we are going to get to in our station black-out program. It wasn't included here because we really didn't have the resources to expand the reactor safety study type of analyses that much, but we recognize that.

MR. EBERSOLE: I think that will also be plant-specific very highly, so a generic study is likely to be of no value.

MR. BARANOWSKY: I think what we do is look at a spectrum of conditions and determine whether or not plants on the high or low side of the spectrum need to make improvements in that regard.

MR. LIPINSKI: In the last diagram, I conclude that the BWR cannot stand station black-out because of the AC requirement on the residual heat rejection system.

If I recall, up to where the suppression chamber reaches questionable characteristics --

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. EDISON: Is your question whether it can withstand a black-out lasting longer than 27 hours?

MR. LIPINSKI: Well, two hours, according to your report. There was a number in here that went with the loss of the system, saying the suppression pool reached peculiar conditions at two hours.

MR. KOLACZKOWSKI: We did include the two-hour case, recognizing that that is a study, and there has been a lot of analysis done on the ram's-head discharge devices, and I think those are all being converted over now. But I think some of the analyses have shown if you still have the ram's-head device, that you may run into problems, more in the two, three-hour timeframe, rather than in the longer timeframes, and that part was included.

Okay, now that we have the accidents, we have quantified the failure probability of the DC system, and as far as other system failures, we are taking that, of course, primarily from the RSS and study.

(Slide.)

We then proceeded through the steps to perform an accident sequence analysis. The first thing was to start with a shutdown cooling fault trees which have been briefly described by Mr. Fedele earlier, and restructured them to contain separate branches, but a different initiating event that we wanted to look at, and also make sure that the structure coincided with the accident sequences that were identified and which we wanted to include in the analysis from the event trees.

We then took those shutdown cooling fault trees, and using two computer codes identified the various failure combinations that could lead to loss of shutdown cooling and possible core damage or, in other words, minimal SEP, and then quantified those minimal SEPs using a SEP computer code which has some routine similar to the sample code that was used in the RSS.

We then combined the failure combinations which fit the accident sequences depicted on the trees, and then took the dominant accident sequences, and again using the SEP computer code, we put in the median failure probabilities and the uncertainty factors and the various elements that made up the minimal SEPs, which in turn made up dominant accident sequences.

(Slide.)

Okay, the next series of slides is essentially going to show you the results as they came out from that computer analysis. This is a summary of the PWR accident sequence probabilities; again remembering that we are talking about within the minimum DC power system.

There are a couple of conclusions that can be drawn with regard to the results.

First of all, what you see on the right-hand column is the median failure probability for the accident sequences that comes out of the computer analysis.

I would not put a lot of emphasis on the decimal place there -- on the second significant figure.

What you see here is that, first of all, it came out that the common mode failures that we have been talking about all along, again those two major categories could be a significant contributor to the overall core damage probability as analyzed in this study.

Secondly, we see that other DC-related accident sequences -- for instance, these down here, appear to be at least comparable to other accident sequences which could lead to loss of shutdown cooling and possible core damage, and yet contain no contribution from a DC failure, and so it was primarily on this premise, and on the fact that these are indeed our best estimates as to what the sequences are, where they lie in terms of probability. It was on the basis of these results that eventually our conclusions and recommendations came about.

There is another factor to consider.

(Slide.)

And due to some of the recommendations in the Lewis Committee report, among which it was recognized there are uncertainties in these analyses and they should be properly documented, we did so, and if you plot the dominant accident sequences along the horizontal axis here -- in other words, each one of these represents a sequence, each one of the sequences you saw on the previous slide, and then look at the accident sequence probability and the range that that probability could exist, based on the uncertainties -- the uncertainties that we incorporated into our analysis, which include not only statistical, but also some engineering uncertainties and the like, then this is the kind of range that you get on where the probability of each sequence could lie.

As you can see, many of them are two and three orders of magnitude.

Again, however, our recommendations and conclusions are dependent on the fact that we are looking at our best guess, and on the basis of that, that is how we drew the recommendations of the report. But there are some large uncertainties to be considered before you draw the conclusions of the report.

(Slide.)

Okay. Quickly, then, to the BWR, because it's a similar kind of thing. Again here is the dominant accident sequences, and we have kind of come up with the same types of conclusions that the common mode failures could be significant contributor, and that other failures leading to loss of shutdown cooling and contain a contribution from a DC power failure appear to be at least comparable, and no worse than other sequences which lead to loss of shutdown cooling, and have no DC contribution.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

Again, the uncertainties kind of ranged in the same magnitude as the PWR.

(Slide.)

Okay. Based on the fact, then, that the common mode appeared to be a very significant factor that needed to be dealt with, we did improvement analysis in which we looked at various improvement features that we might add to the minimum DC system, and tried to assess what sort of improvement we could possibly expect in terms of unreliability of the DC system. If we took each one of these improvements and applied them one at a time, all the various combinations have been looked at down below.

The improvements came from the fact that, first of all, we wanted to look at things that are currently being done in actual operating plants today. That was one source of where the selection came from.

Secondly, we also wanted to look at improvements that would affect either one or both of the two major categories of common mode failures that we identified; again, those being either the loss of offsite power -- or I should say loss of AC, and put to the chargers, and both batteries being unavailable as one category; or look at improvements that might instead help the operational or test-and-maintenance types errors which we saw, based on our LER review.

So what you see here is a summary of that improvement analysis and the expected change that we could anticipate, that

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

you might be able to achieve in unreliability of the DC system, if you indeed provided the improvements shown.

I might just mention that the very last item here, 4, 6 and 7, is actually the recommendations of the report. They consist of eliminating the buss tie-breaker, improving surveillance, and improving maintenance and testing techniques.

(Slide.)

The last step was to --

MR. RAY: Question:

You point out that it's 5×10^{-6}. It seems to me that item 2.C gives you approximately that.

MR. KOLACZKOWSKI: Oh, yes, that's true. You would get roughly the same kind. The reason why we made the last item, particularly the recommendations, is that it appears as though you could get essentially as much improvement through more, shall I say, administrative type or procedural type of improvements, rather than requiring a design change.

MR. RAY: And the hardware there, of course, is less.

MR. KOLACZKOWSKI: I'm sorry?

MR. RAY: The hardware combination is less.

MR. EBERSOLE: If I want to cull out the intrinsic softness of administrative controls in the first instance, in the absence of rigid, as we well know now, personal controls in both the proper operation mode to tell operators what they should and shouldn't do, I guess you anticipate a fair refinement

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

in the QC of operational controls beyond what we have now.

MR. KOLACZKOWSKI: Yes, I guess that's true. We did not try to specify the specific way that these might be implemented, although through the LER review, for instance, you can see things that have gone wrong by pointing those out. Those would be -- you know, those would be the ones you want to look at in terms of, "Well, how can I improve this?"

MR. EBERSOLE: The case at Indian Point recently where they filled the containment up with water hardly gives confidence in administrative controls. One nice thing about hardware controls is that they are hard physical realities. I don't think your study accounts for the difference in the general categorization of these improvements you are talking about. One is a hard physical improvement, and the other is a bunch of instructions.

MR. EDISON: May I comment on that a little?

I think I agree with the tenor of what you are saying, Jesse. You have more comfort from a piece of -- an additional piece of hardware being there as opposed to depending on management to convey instructions or paper procedures, whether somebody will read them or not.

However, I do think -- to put things in perspective -- that we do need to recognize that when we add additional trains, that it is not guaranteed that that train will function, that that hardware will function.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. EBERSOLE: Sure, that's the other side of the coin.

MR. EDISON: We have done that in the past. We have added redundant divisions, trains, pumps, components, et cetera, and when we analyze it, we presume that gives us that pump that will work, it has a reliability of one, and it does not. That's right, we are finding in many cases that reliability was not what it was anticipated to be by designers.

MR. EBERSOLE: On the other hand, it's more useful than 42 pages of instructions, when he's had a fight with his wife.

MR. EDISON: Well, I would agree with you, an additional train would be more reliable than 42 pages of instruction. I hope we are recommending more than just paper work on the shelf, dusty books.

MR. KOLACZKOWSKI: Okay. We entered some sensitivity analyses to see what effects may be differences in plant design or even differences in the unreliability of some of the systems that we looked at and were modeled based on the RSS plants, to see what effect those differences might have on the analysis.

The first one again is just kind of taken from the previous slide, that is the approximate reliability based on the study showed for the minimum DC system, you would have an unreliability of something like 2×10^{-4}, and if you ran down the improvements that we showed on the last slide, where it said it appears as though you could get at best maybe two orders of magnitude change.

And if you do that, you would change the total core damage probability 4×10^{-4} that we have been bantering around by roughly 50 percent, and you would reduce it by that much.

On the other hand, based on improvements 4, 6 and 7, again, the recommendations of the report, if applied with care and recognizing the kinds of failure modes that we identified in here in trying to correct those, that you can get most of that change in core damage probability by using those techniques.

We also looked -- this is just a sample, by the way, we did some other sensitivity analyses than these, and they are all shown in the report -- but we did look at some others, and I think one of the things that some of the entries here point out relates back to the questions earlier as to where would -- you know, where would you put this million dollars and that kind of thing.

I think this just serves to show that you can get some major differences in core damage probability if you don't look at the unreliability of your shutdown cooling systems themselves independent of the DC contribution, and I think the sensitivity analyses also point that out.

(Slide.)

And again, similarly for the BWR, it's just a sample again of some of the sensitivity analyses we performed, and you come to a similar type of conclusions.

Unless there is any further questions -- I don't know whether the NRC or anybody else has any concluding remarks, or if we are over with the presentation at this point.

MR. RAY: Well, seeing no further questions -- did you have something, Mr. Edison?

MR. EDISON: No, I don't, unless Mr. Baranowsky has a concluding remark he would like to make.

MR. BICKEL: I did have one. One of your recommendations I didn't understand. I talked with, I guess, Jesse before. It was recommendation No. 2. If you could spell it out, it has to do with the use of inverters or adding an uninterruptible power source, or whatever you want to call it, and it is not completely clear in my mind if you are talking or using the output of this device for throwing breakers, you know, using AC-controlled breakers or what.

Could you elaborate what that recommendation meant?

MR. KOLACZKOWSKI: Essentially what we are saying is from your offsite power source, you would have an AC supply coming to your inverters, and that would be the normal means by which you would get your vital AC and perhaps even DC.

MR. BICKEL: It was the word "control power" that got me. Do you mean like power for --

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. KOLACZKOWSKI: 120 volt AC for initiation of the shutdown cooling systems, for instance. We are talking about the logic, that kind of thing.

Of course, in addition to that, you have your pump power which is typically 40 volts or something like that.

MR. EBERSOLE: You're talking about going to AC control?

MR. KOLACZKOWSKI: That's right. AC control is your primary source.

MR. EBERSOLE: Normally the inverter would have the alternate of a switching source.

MR. KOLACZKOWSKI: What we are including in that recommendation is the fact that there would be a switching mechanism in the inverter such that if you did lose the offsite power source and switch over to the DC --

MR. EBERSOLE: In that connection, the inverter is put in there and then connected to what is popularly called a fail-free buss to provide a continual 60 cycle wave so you don't interrupt certain functions. When you look at these hard, the only thing that critical is the computers. Most of the stuff hooked to that buss ought not to be hooked to it in the first place.

MR. KOLACZKOWSKI: Your point is well taken. I think you also know that the charger would get a major improvement in the DC reliability if you included that.

MR. EBERSOLE: I think that buss is vastly overused in general for equipment. That ought not to be on it.

MR. BICKEL: The one thing that hit me -- I was a little bit confused by my general feeling about inverters, just from looking at LERs and reports and all that, that the one thing that they really seemed to do when you use them in an uninterruptible power source is they can't interrupt.

(Laughter.)

And the thing that bothered me when I saw it was I thought I cannot believe that they are commending that you are going to use this now for controlling breakers in the switchyard, because that is just as bad as the problem we had this morning of having the DC buss fail and then not being able to move the AC breakers.

The DC buss, at least from what I have seen, is fairly reliable, and when you put an inverter in there, it's like you were adding a new source of unreliability. I just didn't understand what was being recommended here.

MR. EBERSOLE: I don't either.

I think in imposing an inverter to what was an ordinary DC circuit is just adding a complicated feature to the control circuit. Of course, it does permit you, if you help design the receptor in the control room, to take a switching transient, then you could use AC if you had it at some place.

MR. BARANOWSKY: If I could comment a little bit on it, we recognize there is some problem with the use of this

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

so-called uninterruptible power supply.

(Laughter.)

And I think you found, first of all, that there was not a great improvement in the overall system reliability by using that option.

On the other hand, we know that there are plants that do not use their DC power directly and rely on AC power, in the form of 120 volt AC power, through inverters in which they use only the batteries to supply a back-up, should that AC power supply become unavailable due to a loss of offsite power. Inverters are not 100 percent reliable nor 100 percent unreliable. And you get somewhat of an improvement for one particular scenario with the DC power failure, and you get no improvement in the other.

That's all I can say.

MR. EBERSOLE: As a last item, I would like to ask this:

With these two-train DC systems, and they have 40 or 50 circuits taken off one DC buss, and taken out into a hostile environment, which might be the containment, turbine hall, or whatever, and I have a comparable number of circuits off the other bus taken into the same region; I am not clear in my own mind what sort of separative requirements you have to these non-1E circuits drawing their power from 1E sources.

Does Reg Guide 1.75 require these be identified as associated circuits? Would there be physical protection to permit those from being continued?

MR. KOLACZKOWSKI: That is true.

MR. EBERSOLE: But they can enter a common hostile environment and be unprotected, such as for fire or whatever, or the containment?

MR. ROSA: They have to be considered associate circuits, which means they maintain the same separation as the safety-related DC.

MR. EBERSOLE: On the other hand, they don't have any environment control which are required of the 1E circuits, such as protection from fire, floods, by pressure in the containment, humidity, or anything else. They are non-1E, remember.

MR. ROSA: They are non-1E, yes.

MR. EBERSOLE: And that's the common link. Do you follow me?

MR. ROSA: I think I follow you.

MR. EBERSOLE: I am regenerating the transfer, except I will admit it would take 2E series.

MR. ROSA: Associated circuits under Reg Guide 1.75 are required to be Class 1E all the way down to the end.

MR. EBERSOLE: Including environmental protection?

MR. ROSA: Yes.

MR. EBERSOLE: What do you do about the switchyard circuits that run out through the turbine hall and the non-seismic buildings and have no rigid fire controls and so forth?

MR. ROSA: Now that's before the imposition of Reg Guide 1.75.

MR. EBERSOLE: I'm talking about present day.

MR. ROSA: You are right. Under the previous requirements, we depended on the Class 1E circuit overcurrent protection devices to provide isolation in case of a fault.

MR. EBERSOLE: Thank you.

MR. RAY: Thank you, Mr. Kolaczkowski.

I have a couple of residual points. You were historically in the early stages of provocation, if you will, for such a study. Do you have any residual concerns? Do you think this gives you the assurances that you asked when you originally proposed that a study be made of the reliability of DC power supply?

MR. EPLER: Well, I guess I'm sort of overwhelmed with the enormous amount of material, things that the operator has to worry about, the designer has to worry about, and I continue to feel that we have been for a long time pretty close to the end of the road going down this path. But it seems to be interminable, the problems that keep coming up.

I would feel much more comfortable if we could look at the consequences rather than to try to fix all of the details. I think my position has been somewhat reinforced. I believe I was impressed with one of the earlier sheets here, if I can find it quickly, which listed a large number of items contributing to system failure that would need to be corrected.

There is an enormous number of them.

I don't find it right away.

But I am also impressed that there is not any dominant mechanism. Therefore, we would not fix any of them.

MR. RAY: By following this route?

MR. EPLER: Yes. We read that the DC buss contributed 50 percent to residual heat removal, but we don't have minimum systems. We find it actually contributes 5 percent. 5 percent does not encourage the -- instead of just 5 percent, you have to fix 20 of them to get 100 percent.

I think anywhere you turn, you have to find there is not any dominant contributor. That's why there is not any big fix necessary or possible.

I say I think we are at the end of the road.

MR. RAY: Can I conclude from that, that if I could go back to the measure of Dr Bickel earlier in the morning, if you had a million or a multi-million pot to spend to improve reliability, to prevent coremelt and so on, you would spend it on something other than DC system?

MR. EPLER: I would like to spend it somewhere where I could fix all of these things, most of them with one fix, rather than to try to fix an astronomical number of small things.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. EBERSOLE: What would that be, Ep?

MR. EPLER: I still feel the residual heat removal system is what we have to have.

MR. EBERSOLE: A dedicated system, that would embody its own --

MR. RAY: Completely self-sufficient?

MR. EPLER: And we would have to worry about the power supply. We would also have to consider how frequently it needs to work, and therefore a lower level of reliability might add a great deal.

MR. EBERSOLE: That would be in a mitigating context. I couldn't help noticing all the way through here that they operate with so-called defense in depth.

MR. MATHIS: Jesse, we spend most of our time talking about mitigation, and very little on prevention in total.

MR. EBERSOLE: Right. But on the other hand, you can never guarantee through the preventive route that you haven't left some holes.

MR. MATHIS: That's true.

MR. EBERSOLE: So you cover them by mitigating.

MR. MATHIS: But if you don't try and take care of prevention, you ease the burden you are going to put on the mitigation.--

MR. EBERSOLE: You do what you can, and when you are through, you say, "I am not perfect," just like it was at Browns

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

Ferry.

MR. MATHIS: Well, look; we are never going to be perfect.

MR EBERSOLE: No.

MR. MATHIS: The zero accident, zero release concept just has to be realized as an unachievable, and we do our best to get somewhere.

MR. EPLER: Since you asked me, I think I would like to add that indeed we would like to reduce coremelt probability. However, we believe that we have a very good figure for that, which means maybe one coremelt in the life history of all light-water reactors. But we seem to have events occurring at 100 times greater frequency. Media event.

MR. EBERSOLE: What did you call that?

MR. EPLER: Media event, three-ring circus. The Goldbergian cascade, which occurred at about 100 times greater frequency than that, and it's going to dominate the business.

Therefore, we have an urgent and immediate problem of reducing the frequency of Goldbergian cascades which necessarily lead to coremelt. They simply get the pregnant women out in the streets evacuating the premises at a higher frequency than we want.

I think that is the urgent and pressing problem.

Now how does this relate to the health and safety of the public? Well, it relates to the hazards of evacuation as

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

ar24

well as other things. So I think that's the problem.

MR. RAY: I don't want to mean words in your mouth, Ep, but if I can summarize your feeling, I'll go back to what I said earlier:

You feel there are more fertile areas in which to spend the major investments to improve the probability of avoiding coremelt, and your specific feeling is it is a dedicated heat removal system.

MR. EPLER: I do, indeed.

MR. RAY: Completely self-supporting.

And, Bill, I get an impression from your comment that while you support that viewpoint, you still feel there should be a balance of both preventive and mitigative efforts in such --- provisions for such efforts?

MR. MATHIS: Well, I think that's right, Jerry. For example, if we still had those tie-breakers in our DC systems, it's pretty obvious that it should be eliminated. Well, that doesn't cost you anything, basically.

The other thing we haven't really touched on, and that is that the other two recommendations pertain to improved preventive maintenance and the revised test and maintenance procedures.

While these are things that don't cost money, it just takes a little attention and some thought, and to me it is one of the areas that is typical of the kinds of things that need to be improved because fundamentally a battery system should not be tough to maintain and keep up in good shape with just a little attention.

But I think people take it for granted that the things are going to work, and therefore they become complacent and don't pay enough attention to the test and maintenance procedures, and here is a protective area, I feel, again, it's very cheap.

MR. EBERSOLE: That only covers the battery. We have seen where we have emptied them of parasitic loads and everything. It doesn't cover for that.

MR. MATHIS: Well, of course, that's the other thing. A parasitic load problem is one that I am sure individual plants need to give some attention to. I don't know the generic nature of it, I mean how great it may be, but I'm sure there is probably a lot of designs and installations that have a real serious problem.

MR. RAY: An implementation of these recommendations would certainly correct many of the outlying plants, if you will, in terms of net range of 1 percent to 50 percent contribution.

MR. MATHIS: Well, it would certainly improve the reliability, and I would hope we would get it from where we feel now it may be 5 percent down to the 1.

MR. RAY: Jesse, if I may turn to you, you have been perhaps the agitator, if I can use that word with quotations

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

around it, for improved reliability in DC supply. Do you have any residual feelings, after having surveyed this study?

MR. EBERSOLE: I think I will endorse Mr. Edwards' approach to this. We can cure one aspect of our safety problem by upgrading and improving the DC system. I would personally endorse n^ using the soft technology of administrative controls, but rather [illegible] my work in hardware. Maybe it's just because I have an intrinsic distrust of operators messing things up, like we do in a scram system. We don't tell the operator to hand-scram the system.

MR. RAY: And then address --

MR. EBERSOLE: Yes. However, I would not want to pursue that so far as to depreciate the opportunity. What we all ought to do is do an integrated study of the shutdown heat removal system and approach, I hope, the inclusion of a dedicated system of that sort in a plant in a purely mitigative capacity with infrequent challenge.

MR. RAY: Okay, I didn't mean to neglect you, Dr. Lipinski, if you have any amplifying remarks to make.

MR. LIPINSKI: No.

MR. RAY: Dr. Davis?

Well, then, if I could perhaps summarize this, subject to what the notes will correct me with.

We feel -- and now my own personal observations -- I think, gentlemen, you have made a real contribution to the

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

background available to the industry and the regulatory organizations by this effort of a generic study.

I think it is a milestone, if you will, in this area and you are to be congratulated for that. And I would like to say that perhaps a consensus here of our subcommittee and consultants is that, one, we feel that in spite of this, if you will, that major investment requirements of the industry might best be made in the area of changes -- other changes, if you will, underlying, perhaps I can say, for relative importance providing residual heat removal systems.

I would like to name two. However, the suggestions or the recommendations or the outcome of this study in the area of improved procedures, improved maintenance, improved testing, et cetera, certainly should be implemented. Do we all feel --- so those are two major conclusions we would like to expound.

Would you have any objection if I summarized these in terms of a report to the main committee in this area, in this manner?

Okay. Well, we will be certainly -- by the time --- I don't know how quickly I can do this, since I am on vacation concurrently with this effort.

(Laughter.)

But in the remaining week of my vacation, I will attempt to come to the main committee meeting in February with a draft which certainly the subcommittee members may see, and

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

while you may not be able to influence what is said at that meeting, I think something is expected of us from the viewpoint of a statement at that meeting. I certainly will make available to you whatever is finally said, as consultants, through the mail at that time.

I would like to ask, too, whether or not you feel that this subject or the subject of this report, this effort, is of such importance that presentations for the interest of the main committee would be in order. Would you feel I should recommend that the main committee in one of its future meetings -- probably not February, because I think that's pretty well set in concrete -- be added to the agenda for future meeting?

MR. EBERSOLE: I think it would be interesting to present the implications of the electrical systems failure being a major contributor to the overall safety problems in the plant, particularly as regards the research effort; whereas there is hardly a dollar spent in this area, although it is a major contributor to a safety problem.

MR. RAY: I respect your comment, Jesse, but that doesn't answer my question. Would we want these gentlemen to make a presentation to the main committee? Perhaps reduced in time and content.

MR. EBERSOLE: I would say a shortened version.

MR. RAY: An hour?

MR. EBERSOLE: An hour or so.

MR. RAY: So, therefore, I will prepare the kind of report I mentioned to you a moment ago, be very brief, and recommend that because we feel that it is such a milestone in progress, that the main committee should give it approximately an hour at a future meeting.

Would you gentlemen have any objections to that?

MR. EDISON: None.

MR. RAY: Might I ask what you plan to do now with this report, having developed it? It's in the status of a NUREG, and will be issued as such, if it hasn't already. What will be done to implement any of these things beyond that?

MR. ROSA: The Power Systems Branch -- I believe I mentioned it before -- will, priorities permitting, and I think this is high priority, begin now to draft revised requirements for DC power systems and will base those revised requirements on the recommendations of this report and the sensitivity studies and report on the --- will attempt to get into the revised requirements those features in excess of the present minimum requirements which we are already getting, anyway, in order to formalize that, and any significant operating experience that might be relevant.

MR. RAY: When you say requirements, I assume you mean regulatory requirements, not just reviewers' attitudes?

MR. ROSA: Regulatory requirements. Yes.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. EBERSOLE: I wish you would include in your studies comparative analysis of the sensitivity and effectiveness of the hardware improvements versus administrative improvements. Do you follow me?

MR. ROSA: Well, for this effort here, to implement what this report seems to say should be done with regard to improving the present requirements, I am not going to go beyond what the report contains. I cannot do that with the resources available to me.

Now, of course, I believe the ACRS will have an input to what finally evolves here, and I hope that what finally evolves will not be very long in coming.

MR. LIPINSKI: Your decision to present this to the full committee, I think, is good, because the committee has recommended that quantitative methods be applied to try to arrive at decisions such that this study now has tried to quantify what is involved in the particular two members, namely Drs. Okrent and Lewis, would be, I think, particularly interested in the results of this work.

MR. RAY: That's a very good point, Walter, and I will make sure to mention it in my response to the main committee's interest that point.

There will be contained in that the analyses on the scram system at boiling water plants prior to the Browns Ferry Plant, and the revelation that extensive analyses showing extreme reliability can be made entirely --

MR. LIPINSKI: Well, I'll take you back to the very first day that we started ATWS. The first meeting was at Argonne National Laboratory. The subcommittee met there. General Electric came in, they made their initial presentation. 5×10^{-15} probability of failure. But then that posed the question, where does the water go in the scram? And they said, well, to this tank.

I says, what happens if the tank is full? The rods don't scram. How do you guarantee the tank will not be full? We have a level alarm on it. If the tank is filled, the alarm sounds and by administrative control we empty the tank.

Then they went to the dual scram-headers. Okay. Well, that supposedly solved the problem, except now there is a fault in design that allows the header to fail.

MR. RAY: To the gentlemen of the NRC Staff, we are very grateful for your presentations this morning. I think they were very, very effective and high quality. Thank you very much.

VOICE: Mr. Chairman, may I say something?

MR. RAY: Will you identify yourself, please, and make it brief.

MR. BAXTER: Baxter, Yankee Atomic Electric Company.

I would caution before we get carried away with the conclusions of 0660, this report, its findings and its

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

conclusions are very limited to the DC configuration that has been assumed in the beginning, and it should not be applied to all the DC systems, and I say this because it is so easy to get carried away and say these are the conclusions of 0660, apply them across the board to all DC systems.

For example, there were certain recommendations that switchyards should have their own batteries; diesel generators should have their own batteries. That might be true for the DC configuration assumed.

Thanks.

MR. RAY: I think maybe this admonition would be a good one for the Staff to bear in mind in how they couch, if you will, the regulatory requirements that you have in mind.

MR. ROSA: We intend to take this into consideration.

MR. RAY: Thank you for your comment.

Okay, this meeting is adjourned then until 2:00 o'clock.

(Whereupon, at 12:55 p.m., the meeting was recessed, to reconvene at 2:00 p.m., this same day.)

- - - - -

end AR
fls

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

AFTERNOON SESSION

(2:05 p.m.)

MR. RAY: We would like to resume the session with a discussion of the topic, "Consideration of the Loss of AC Power as a Design Basis Accident." On the subject, we will hear from Bob Fitzpatrick of the NRC Staff.

MR. ROSA: Pat Baranowsky has prepared some information describing what we're planning to do on the Task Action Plan A-44, Station Blackout, which --

MR. RAY: I see. Then my notes are wrong. It's Pat Baranowsky?

MR. ROSA: Yes.

MR. RAY: My apologies.

MR. ROSA: So he will present that limited presentation that he's got available, and we can talk from there.

(Slide.)

MR. BARANOWSKY: I guess you know who I am, but I am going to be talking about the program that the NRC is following with regard to resolving the issue known as "station blackout," or Task A-44 in the unresolved safety issues list.

I am NRC's manager of that program.

(Slide.)

At this time, we've tried to define the issue as follows: Is the loss of all AC power at nuclear power plants a relatively high probability event? And are the risks posed

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

by a station blackout or a loss of all AC power unacceptable?

(Slide.)

With that definition of the issue, we have formulated an approach to this unresolved item. We would like to evaluate AC power reliability at nuclear power plants, and cost effective improvements.

We would like to look at station blackout accident sequences and consequences, and then determine of course the risks associated with those accidents associated with the loss of all AC power.

And we would propose to develop our recommendations based on comparing, again, the risks associated with the station blackout accident to those of other nuclear power plant accident scenarios. Or, if available, we would compare it with an NRC safety goal, for which I understand there is some effort underway now, and at least an interim goal is due out in the near future, probably before we would complete this work.

(Slide.)

MR. RAY: Who is developing that goal, Pat?

MR. BARANOWSKY: I think the responsibility might be in the Office of Policy Evaluation. I know that our division, the Division of Systems Reliability and Research has some input to that. I don't know the person who specifically is heading up that work, but there was a NUREG published, either NUREG-0735 or -0739, which describes the NRC's program in that effort.

As I recall, there is a proposal to put up a -- either an interim or strawman type of goal by around mid-calendar year 1981. So unless the schedule has changed, that is when I expect to see something come out from the NRC on that. I don't know whether it will be quantitative or qualitative, or a combination of both. I'm sure it will have input in both directions.

MR. EBERSOLE: In response to your first two questions that you started with -- Is the loss of all AC power at nuclear plants a relatively high probability event? This has been answered at least to some degree by WASH-1400, and the answer is "yes."

If I recall the arithmetic correctly, it showed that any given plant over its 40-year life -- I may have an error in my memory here -- displayed an approximately 1 to 100 chance of probability of experiencing a power failure extending beyond one hour, 1 to 100. That's a high probability.

I don't know whether it's any good or not, but whatever it is, in that same study the consequences mitigated by looking at the presumed independence of steam supply systems from feedwater, in the absolute ignorance of the interdependencies between AC and the steam turbine systems which presumably furnish feedwater.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

So there is a standing and conflicting answer to those questions right now. Have you looked at this?

MR. BARANOWSKY: Yes. And one of the reasons we included that question is that this is somewhat of a plant specific problem. In this program, we plan to not just look at a minimum system, but look at the spectrum of designs from the minimum to the optimum. In fact, that's how we expect to develop cost-effective analyses as to what can reasonably be expected in terms of AC power reliability? And where should someone spend their money? It is, I think, a significant step beyond what we did on the DC power work.

MR. EBERSOLE: Yes, it would be.

MR. EDISON: Could I interject there, Jesse? Would you repeat the number you are quoting?

MR. EBERSOLE: I am depending on my memory. I seem to recall that the probability of exceeding a one-hour total AC power outage, factoring in the 40-year life of a plant, was about 1 in 100 per plant. That is including most units. This looked at grid reliability, and diesel failure to start and so forth.

MR. EDISON: Oh, no. That's way too high.

MR. EBERSOLE: Have you looked at it yourself?

MR. EDISON: Yes.

MR. EBERSOLE: Okay. Given a 40-year plant life, what is the probability that it will suffer a power outage of

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

all AC beyond one hour, in your --

MR. EPLER: Off site?

MR. EBERSOLE: All power.

MR. EPLER: All?

MR. EDISON: You're talking about all power?

MR. EBERSOLE: All AC power.

MR. EDISON: And of course it is plant specific, but the kinds of numbers that have been tossed around are a .2 probability of losing off-site power; and then for a couple of diesels, another 10^{-3} or $^{-4}$.

MR. EBERSOLE: I magnified it by a 40-year plant life.

MR. EDISON: So that you're talking something like 2×10^{-5} per year. That kind of a number, ballpark. So that if you're talking 40 years, I still don't see you getting to 10 to the --

MR. EBERSOLE: You think that's too high? Well, I'm drawing it from memory.

MR. EDISON: It sounds too high. But in addition, I would like to point something out. WASH-1400 of course was done in the 1972-1973 era. We have learned a lot since WASH-1400, and there are some uncertainties in some of these numbers -- the diesel reliabilities and the off-site power numbers.

For example, when we talked to one plant about their diesel experience and confronted them with what we thought was the operational data, they said: Oh, wait a minute. We started our diesels five times as often as you guys are giving us credit for. And we checked with another plant, and they said it was three times as often.

So there is some concern that there might be factors of three or five floating around in the woodwork that are real factors that the analyst doesn't know about.

One of the things that this A-44 program was going to do is try to root those out.

MR. EBERSCLE: Well, what would you say your present understanding is about given -- I'm looking at it from an investor's standpoint -- what probability in that plant of suffering a sustained -- by that, I mean a one- or two-hour power outage, on the average, across the 40-year life would you say you understand that to be now?

MR. EDISON: Yes, and I would have to say that the answer is a spectrum of answers, depending on the plant.

MR. EBERSOLE: But what's the -- You're telling me that WASH-1400 is no good.

MR. KERR: Jesse, the gentleman up here was supposed to make a presentation on this subject.

MR. EBERSOLE: Yes.

MR. KERR: Why don't we listen to him --

MR. EBERSOLE: He went by that.

MR. KERR: -- and see what he has to say.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. EBERSOLE: I don't think you were going to develop this topic, were you?

MR. BARANOWSKY: The specific area that you're talking about now is actually a part of our program. We recognized that WASH-1400 was an analysis of two plants, using some industry-average data for which we have information available that indicates, just using LERs and some assumptions on maybe monthly testing, may not be adequate to analyze and determine the reliability of AC power supplies.

So we are actually attacking the problem on two fronts. That is, we want to assure that we know what the probability of this event is with some reasonable accuracy; while, at the same time, looking at the consequences of the event such that if our analysis of the probabilities confirms that this is a relatively high probability event, we can understand the consequences and recommend appropriate fixes, so that we understand the whole problem. Okay?

Rather than just starting off and saying: WASH-1400 had it all, or some other unknown study which is not based on a good foundation in terms of data from plants, predicts some unreliability of the AC power supplies, I don't think that would be quite right. Because we could really do that on any topic, in addition to AC power.

MR. EBERSOLE: Okay.

MR. BARANOWSKY: So, instead of just saying let's look at the AC power reliability, then a year later come back and say: Now let's take a look at the consequences. We're going down both paths at the same time.

MR. RAY: Dr. Lipinski?

MR. LIPINSKI: In considering the loss of off-site power, are you going to use a nation average? Or are you going to try to develop numbers that apply to specific regions?

You mentioned you were looking at Florida, so in that particular case I assume you have a number that applies to Florida; but what about the rest of the country?

MR. BARANOWSKY: I think what we would like to do is come up with some criteria that take into consideration the plant-unique aspects associated with this problem, as well as the generic implications. I can't tell you what the final formulation in terms of our probability equations would look like for loss of off-site power, but I already know the nation average. I am paying some people a lot of money to tell me more about this problem than just what the nation's average is.

MR. LIPINSKI: Well, are you going to get it by a region average?

MR. BARANOWSKY: I don't know whether --

MR. LIPINSKI: Because a nation average --

MR. BARANOWSKY: -- it's possible to do it by region, or by site, but what we will do is develop recommendations based on analyzing information that we think is verified

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

as much as possible from plants, considering regions and all the factors that go into causing losses of off-site power; rather than just blindly saying there have been 10 losses of off-site power in 100 years. I think we want to know why they occurred, and if there are some plant-specific design considerations that go into this, or region-unique considerations, and we would hope to have a conditional probability in the long run. I don't know exactly how definitive those conditions will be, but we will try to break it down better than just the industry average.

MR. LIPINSKI: I had a piece of information that kind of relates to what we're talking about. I haven't been able to confirm it. But in talking to a computer simulation company, they made reference to having delivered a 1000-amplifier analogue simulation to Purdue University, and I was told that that was being used on some type of grid simulation problem for DOE.

MR. BARANOWSKY: We plan to include in this program contacting other government agencies regarding on-site and off-site power supply reliability. I think if you look at the data that is associated with loss of AC power plants, you'll see some of it has to do with grid stability, a lot of it has to do with other things like local weather conditions, faults within the plant. And what we would want to do is separate these things out. And if grid stability turns out to

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

be the major factor, then we would look into that type of an assessment. If it turned out to be a lesser factor, we would want to divert our resources into the areas where we could get more information.

MR. KERR: What do you think is the uncertainty with which you now know the result? Is it a factor of 10? Or a factor of 100?

(Pause.)

What I am getting at is: How much money are you going to spend to decrease the uncertainty? And how much of the decrease will you achieve? And if the answer is, "I don't know," I'll accept that.

MR. BARANOWSKY: I don't think it is as much uncertainty as it is in pulling out the conditional aspects to the probability. We know that we have plants that on the average have about a .2 loss in off-site power -- some higher, some lower.

We want to know why some are higher and some are lower; and are there trends that we can track.

MR. KERR: I am an academician, and I think your information has academic interest. But one also needs to ask: What is one going to do with the information? And if you find that the existing uncertainty is a factor of 10, let's say, I'm not sure that's relevant. Maybe it is.

MR. BARANOWSKY: We're not really going into the uncertainty in that respect.

MR. KERR: Well, you're spending money to decrease the uncertainty with which you know something, I think.

MR. BARANOWSKY: Okay. Relatively speaking, that is the smallest part of our program, if you're talking about off-site power reliability.

MR. KERR: Well, I don't know what else one would be spending the money for. If one has a certain amount of information, presumably one is trying to increase the quality of that information.

MR. BARANOWSKY: Yes.

MR. KERR: Which to me means decreasing the uncertainty in both qualitative and quantitative senses.

MR. BARANOWSKY: Okay. The uncertainty in that regard is: If the average is .2, the highest we have observed is maybe 1 per year, and I doubt that whether it is .2 or 1 per year makes a big difference.

On the other hand, we have plants also that are exhibiting probabilities for losing off-site power circuits less than .1. Now I think it would be unrealistic and unfair for the NRC to come up with requirements to exhibit loss-of-off-site power reliability equal to or less than .1 per year, in the same way that we treat plants that have frequent outages.

MR. KERR: No, but it seems to me you can make that

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

decision without any further study. Indeed, you have already said you think it would be unfair.

MR. EDISON: Can I interject for a moment here, Pat?

MR. KERR: This is perhaps not the time to discuss it, but I thought perhaps you had some idea of what the uncertainty was, and now you could decrease it.

MR. EDISON: In my earlier response to Jesse Ebersole, I mentioned that we were talking about numbers like a frequency of .2 per national average of off-site power losses, but numbers like 4 orders of magnitude on the on-site power on the diesels.

So clearly in terms of the probability of this overall blackout event occurring, the large protection is there with the diesels in terms of probability of failure.

MR. KERR: But the nationwide survey of off-site power doesn't really contribute anything to that uncertainty, does it?

MR. EDISON: No.

MR. KERR: Unless I misunderstood.

MR. EDISON: The point I wanted to make here is: The effort is largely focused toward trying to remove the uncertainties on the on-site power losses.

MR. KERR: I misunderstood that.

MR. EDISON: We have a small piece headed for the off-site power?

MR. KERR: So you're not putting much effort on that, then?

MR. EDISON: That's correct.

MR. BARANOWSKY: That would be the smallest part of our program.

MR. DAVIS: Mr. Chairman, a question?

MR. RAY: Yes.

MR. DAVIS: Last year I studied the aux feed system for a PWR, and I was told by the utility that they have been instructed by the NRC to be able to withstand a two-hour loss of AC power. Do you know what the basis for that requirement is? And do you know if that is true for all plants?

MR. BARANOWSKY: I don't know. I wasn't involved in that particular study.

MR. EDISON: I can answer that, Pat. Last year, we did a reliability study of the auxiliary feedwater systems for all of the pressurized water reactors. We made many changes and recommendations, and those changes are in fact being implemented. Many of them have been implemented.

Among the criteria for change, one of them was -- and I wasn't involved in the setting of it; I understand a little about it -- one of them was to try to make the auxiliary feedwater system such that it could run under the circumstances of loss of off-site power for two hours. I think

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

it is related to the steam generator inventory, the time to boil off and the time before you start to get into other unknowns that are off-site, or that are AC-power related.

MR. KERR: Is the answer to Mr. Davis' question "yes," or "no"? Is there, or is there not, a requirement that the aux feedwater system operate for two hours without AC?

MR. EDISON: There is a requirement. And when I say it's a requirement, I don't want to say it's in the regulatory criteria --

MR. KERR: How else can one say it?

MR. EDISON: The requirement has been imposed upon the plants in the form of bulletins, or --

MR. KERR: What does this mean, if it's not done in a regulatory criteria?

MR. EDISON: Let me say, in a formal regulatory Guide, or --

MR. KERR: But the plants have to do it?

MR. EDISON: That's right.

MR. KERR: Even though it isn't a regulation?

MR. EDISON: That's correct.

MR. KERR: I guess I don't understand that sort of English.

MR. ROSA: Excuse me. I could add a little bit to that. There is a RSV position that requires auxiliary feedwater systems to operate -- to have redundant parts, one part of which is completely independent of AC power. Now implicitly, because we require that a battery be capable of performing all its safety functions for at least two hours, including an accident, that implies that the AC independent part of the auxiliary feedwater system should last at least two hours. So that may have grown from that.

(Slide.)

MR. BARANOWSKY: Okay. There are several technical programs going on to provide the information necessary so that we can resolve this issue. We have contracts for technical assistance with several organizations through two different parts of the problem.

The AC power reliability part is contracted with Oak Ridge National Lab, and which they have a contract with JPF Associates, and they are in the process of obtaining an emergency diesel generator consultant.

In that program, we are going to be spending most of our efforts on the on-site AC power system. We are looking for interactions. We will be spending a smaller part of the effort looking at the off-site power reliability and the factors that go into that reliability.

We will be developing types of improvements that are practical in trying to determine the cost of these improvements, and they may include adding diesel generators if the probabilities are sufficiently high. At any rate, we

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

want to bring in the cost and the impact on that particular item, in order to help us --

MR. KERR: This is first an effort to determine what the experience is?

MR. BARANOWSKY: We have to have a good base to start with, is the way we see it.

MR. KERR: And then once you know what the experience is, you will decide whether it is good enough? And by then you will have some sort of goal which will come from some other part of the NRC, probably And having determined whether or not the goal has been reached, if it has not been reached you then propose to design systems which will permit the goal to be achieved?

MR. BARANOWSKY: Yes. I think it is reasonable to expect that the resolution of this issue will involve some AC power reliability requirements, as well as some capability to cope with loss of AC power. But I don't want to have a preconceived notion as to what the solution might be. I think it would be better to let the analyses run their course, and through a review determine their validity.

At any rate, Sandia National Laboratories will be taking a more in-depth look at the accident sequences associated with the loss of AC power. Some of the items that will be covered there were discussed, in fact, this morning in terms of what were the long-term effects of losing AC power? Or how does one cope in the short term in the capability of systems which are independent of AC power? And are they independent of AC power to perform a function of maintaining a cooled reactor core without significant damage?

They will take a look at accident sequences which go into core damage, core melt, and develop a risk profile for us for a spectrum of accident sequences that cover a spectrum of plants.

Some of the specific plant thermal hydraulic response parts that go into determining consequences will be performed as part of the SASA program, which is being managed by the Division of Water Reactor Safety and Research of the NRC, with contracts to the EG&G, OR&L, and Los Alamos.

MR. LIPINSKI: What is "SASA"?

MR. BARANOWSKY: That is the "Severe Accident Sequence Analysis" program. What we are doing is taking the accident sequences that we feel are important from a probabilistic and risk perspective, and asking them to analyze them to be sure that the plants do in fact respond in the manner that we assumed in our probabilistic analysis.

Then they will also be including consideration of operator actions in that particular part of the program, as well as in other parts of the program.

I didn't put together a schedule slide, but we expect to have results by early 1982, and a final resolution, NUREG and so forth, completed by October 1982. In that period, what we expect to do is to come before the ACRS, probably this subcommittee, as results are available to describe what we've found and where we're going, and of course to have some sort of a feedback.

That completes my presentation on the Task A-44.

MR. RAY: Any questions?

MR. LIPINSKI: Yes. Sequoyah, as part of its starter procedures, implemented a station blackout. Have you followed what they did?

MR. BARANOWSKY: Not specifically. We plan to, as part of the program, review various plants that have procedures and determine whether or not they are adequate considering the possible spectrum of events that could occur. But we haven't taken a look at specific plants requirements at this time, except in a general way we know the kinds of functions that must be available given a loss of AC power.

MR. KERR: In your allocation of an appropriate goal for DC systems, I assume that this will be based on some goal that says an acceptable probability of core melt is something, and one must then allocate some fraction of that to power supplies.

Does there exist some sort of committee structure, or some other structure within the NRC that decides on this allocation process, so that some fraction goes to power supplies, and some fraction goes to this, that, and so on?

MR. BARANOWSKY: No. Unfortunately, really the only guidance that I know of available is the Commission's policy statement on the use of risk assessment techniques in licensing, in which they say you can do some relative types of analyses and be very careful when you talk about absolute values and be sure to include the uncertainties.

In terms of a goal, I don't really know of any allocation between power systems and so forth, and I am actually hoping that something will come along before the end of this program that will be beneficial both to this work, and maybe some other previous things.

MR. KERR: Well, in order o take the next step to which you referred, I think, which is to decide whether something needs to be done, somebody will have to decide what fraction of the risk should be allocated to power system reliability. Otherwise -- and it seems to me it's not too soon to be giving some thought to the process that may be used for that purpose.

I would assume that this won't just be true of power supplies, but it will be true of other systems and subsystems, as well, as one begins to apply this technique toward determining whether system performance is acceptable.

MR. EDISON: I understand that there is a Steering Committee for this "how safe is safe enough" question, which

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

steering those people on trying to develop a goal. On the subject of, "well, once you've got a goal, will you allocate it?" let along how you allocate it, how do you allocate it? and whether it will be quantitative is still yet to be seen.

I have talked about this with people in NRR, various branch chiefs, and there is a very strong resistance to having a quantitative requirement in terms of a statistical reliability requirement for systems like auxiliary feedwater, or electrical power, whatever.

MR. KERR: Well, now, did I misunderstand? Because my understanding was that when you finish the study to determine the way things are, somebody is going to decide whether the existing reliability is appropriate -- which means to me, "good enough" -- and if one doesn't have a quantitative criterion, is there another process that is going to be used to determine whether it is good enough?

MR. EDISON: I honestly can't tell you whether the goal committee is going to come up with a quantitative goal or not, or whether it will be qualitative, or a combination. And once they do, whether it will be accepted by the entire staff, the NRR, or whether they will want to question it, challenge it, or find that they can't apply it in practice.

MR. KERR: Are you pointing out to the appropriate committee that a need for such a goal is likely to exist as the status progresses?

MR. EDISON: Absolutely. Our director, Bob Bernero, is on that committee, and he is well aware of the ACRS recommendation to the Commission for such an effort.

MR. RAY: Are there any other questions or observations?

(No response.)

MR. RAY: Thank you, Mr. Baranowsky.

MR. EDISON: There is one other comment, before we close this, and maybe I can direct this to Mr. Lipinski.

We made some preliminary looks at losses of power at power plants around the country. In reviewing the information provided by the plants themselves, and reviewing the LERs, we do not find a large -- a higher frequency of off-site power losses at the Florida plants. A popular belief would be that with the peninsular geography that you might have less of a grid flexibility there, and that the number of losses that are occurring in those plants would be higher than the rest of the plants around the country.

But what we find is that other plants lose their power -- be it tornadoes, cutting power lines, or ice storms, or heavy snows, or some of them are located on ocean coasts where they too have a limited grid -- and that when one looks at it, the deviation is not that large from plant to plant around the country. That is, we don't see the Florida plants way up, and the other plants down. They are right in the pack.

And if one looks at the top 10, we don't see the 3 Florida plants up in 1, 2, 3, and we might only find one Florida plant in the top 10 plants.

MR. KERR: Have you passed on this information to the ASLB that went through this protracted hearing, I presume?

MR. EDISON: Yes.

MR. KERR: They don't accept your information? Or did they just not have it when they published their requirements?

MR. EDISON: I think they did not have that information at the time.

Now there is one more consideration in all of this. It may be that the failure mode of off-site power is important for recovery. That is, tornadoes cutting power lines is one situation that you may be able to send people out to put power lines back up. Losing the grid may be a more difficult thing to recover. So that is a consideration.

But if you're talking about the frequency, I think if you look at the data, at least what we have now, you will find that there aren't any regions that are particularly high for loss of off-site power.

MR. KERR: Well, I guess I don't understand what you're telling me, so let me try to understand it. You seem to be saying that the mode of loss may be important, and that it may be different in Florida than it is in other places. Hence, the

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

frequency of important modes might be different in Florida.

MR. EDISON: That may be. We have not looked at that.

MR. KERR: Now do you know which one of these the ASLB looked at when they reached their -- and indeed, it seems to me, the NRC Staff. Didn't the Staff, I guess in compliance with the ASLB findings, set some requirements on Florida that are different than the requirements that exist in other places?

MR. EDISON: I'd rather not speak for the Staff setting requirements, but I have read the ASLB summary of the St. Lucie hearings. They were primarily -- they looked at all modes, and recognized that the tornadoes and ice storms were not the problem in Florida.

So what they really discussed was the grid availability problem. It makes sense to me that the grid availability problem might be heightened in Florida.

MR. KERR: Well, I guess I don't know the difference between "grid availability" and "power availability."

MR. EDISON: Let me -- by "grid availability," I mean loss of a transmission -- a substation, for example, that could not bring the power to the plant for one reason or another, and which would be very difficult to recover in a short time.

Weather initiated phenomena do lend themselves to some possibility for recovery. That is, if for example the grid covering five states should black out, that's a more difficult thing to recover, and one has a little less control over getting that back, I think, than one has over putting up some power lines.

MR. KERR: But with the information you now have, you would not see any reason for setting different requirements for power systems in Florida than power systems in, say, central Missouri or western Kansas?

MR. EDISON: Not with the information that we now have.

MR. KERR: Thank you.

MR. EBERSOLE: Do you have any feel for the nominal sustained on-site AC power failure that you would experience today? Once every five years? At a station.

MR. EDISON: By "sustained"?

MR. EBERSOLE: I'm talking about long enough to make it serious, like one hour or longer. That's a qualifier, because there will be many outages that you can correct quickly.

MR. EDISON: What you're really talking about is taking the .2 number.

MR. EBERSOLE: That's one every five years.

MR. EDISON: One every five years for a momentary loss, and then looking at how soon we get it back: What's the probability of getting it back? And then multiplying that.

The recovery probability will, as I said -- may be mode dependent, and even region dependent. The WASH-1400 study used roughly a .2 factor for that recovery based on the Bonneville Flats data for recovery, a half-hour to an hour time range. We really have not gone into that, yet, although the TASK A-44 will.

MR. EBERSOLE: Take that number, whatever you want to pick, and then you take as a fixed number 40 years in the plant life as a hard number. You take three units present at a typical one-unit station. The only other part of the problem is diesels starting to run, that reliability. You can do that in a few minutes, the arithmetic on that.

I think that is an unacceptably high failure rate.

MR. EDISON: I think you have to look at an integrated problem there. Let me just mention one factor. That is, if you're talking about a three-unit station, it may be that they can share diesels.

MR. EBERSOLE: Isn't that nice that you've just said that when I said this morning that that's been condemned?

MR. ROSA: If I might respond to that, sharing of on-site power supplies means that there is one power supply that can be swung from one unit to the other. It does not mean that a power supplies that are dedicated to the unit, and the unit needs no more power supplies than those dedicated.

However, there is the capability to interconnect.

MR. EBERSOLE: You mean, in a preferred power context?

MR. ROSA: In a preferred power context.

MR. EBERSOLE: Well, yes, but you're operating --

MR. ROSA: You're operating in an emergency on-site power context.

MR. EBERSOLE: You're so low on the load curve for these big generators that that kind of load is down at the bottom end of 1 percent.

MR. ROSA: I'm not talking about trying to supply full auxiliary loads; just safety loads -- on-site power sources, I'm talking about.

MR. EBERSOLE: From diesels?

MR. ROSA: Yes.

MR. EBERSOLE: By swinging them between units?

MR. ROSA: No, what I'm saying -- what I'm trying to bring out is a distinction between shared on-site power supplies and not shared on-site power supplies.

For instance, at Zion each of the two units is a three-division unit, but there are only five diesels. And one of the diesels swings between the two units. That is a "shared on-site power supply."

MR. EBERSOLE: Yes.

MR. ROSA: However, if each of those two units had three diesels and you had the capability to interconnect diesels

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

from one unit to the other, that would not be a shared system.

MR. EBERSOLE: Yes.

Well, by the way, just as a number to feel with you, what do you consider now to be the start-and-run reliability of diesels to start and run?

MR. EDISON: Well, it's start, load, and run.

MR. EBERSOLE: Start, load, and run.

MR. EDISON: We are examining that number. That number probably I would say it ranges between 10^{-1} and 10^{-3} per diesel.

MR. EBERSOLE: That's mighty good.

MR. EDISON: That's a wide range.

MR. EBERSOLE: I thought it was nearer 5/100ths, or thereabouts. Does that come from industry experience?

MR. EDISON: Well, that's between 10^{-1} and 10^{-3}.

MR. EBERSOLE: Right.

MR. EDISON: It varies from plant to plant.

MR. EBERSOLE: Well, if you put these numbers together and you find that this is a frequent event. Remember, I have compounded it by putting a multi-unit station in.

MR. EDISON: Right.

MR. EBERSOLE: I didn't take the beneficial aspects you just referred to.

MR. EDISON: This question came up in the St. Lucie hearings, and it was discussed in the ALAB-603 report. What

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

the ALAB people said was: Well, St. Lucie here has two units, and they have a couple of diesels at either unit. But they don't have procedures in place to tell them when, under an emergency, that they might use unit one diesels in an emergency for unit two. They acknowledge they're there; the capability is there to interconnect them if they have to have them; but without the procedures in place, they wouldn't give them credit for that.

What I am saying is that when you bring up a multi-unit site, that is a conservatism that is available to operators in an emergency to try to deal -- or they can be available if there are procedures to make things better.

MR. EBERSOLE: I thought in general you were discouraging unit interchange; that you wanted to consider modules. Or am I hearing something to the contrary?

MR. EDISON: No, I'm not saying I encourage it or discourage it. What I am pointing out is that in an emergency and I mean a real emergency, where it's to do something or else, one has a way or an option -- can have an option to try to do something about it, and that is a plus.

MR. EBERSOLE: Yes. Thank you.

MR. KERR: It probably follows that if procedures didn't exist as part of the technical specifications, the plant operator would be fined for doing this. But that is just an incidental comment.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

When you gave the numbers of 10^{-1} to 10^{-3} as the reliability range, did you mean to imply that some plants might be 10^{-1} and some might be 10^{-3}? Or just that the uncertainty in your knowledge, if one looks at a total population of diesels, is somewhere in that range?

MR. EDISON: The uncertainty in my knowledge, and in all of our knowledge. We have seen data reports on diesels, but when you start to deal with the real nitty gritty of the data to see what really is a failure and what's not a failure, and try to reinterpret the data, the uncertainties are there of that 10^{-1}, 10^{-3}.

Let me throw an example out. There is a recent diesel data report out -- I think it is NUREG-1352 -- that claims one-sixth of all the diesel failures are common-mode failures.

Now we have dug into those individual 50 so-called "common mode failures," and only a handful of them are really multiple diesel failures. All the rest of them are single diesel failures that look like they had a potential for common mode. There is a difference between real multiple failures as operational experience and a single failure that looks like it has common cause potential when you're dealing in the statistics of common cause failure.

So it might be a factor of 10 lower, in terms of the common cause failure rate. Now I'm just talking about data

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

analysis now. And the same sort of thing with single failure, single unit failures. We need to look very carefully at just what is a "failure" and what is not. We need to define it properly and get a better handle on these numbers.

In the meantime, people walk around saying 10^{-2}, 10^{-3}, and we want to try to clear that up in this Task Action Plan A-44, since the diesels are four of the five orders of magnitude that we think are, roughly speaking, are available to protect against station blackout.

MR. LIPINSKI: Mr. Chairman?

MR. RAY: Yes.

MR. LIPINSKI: In NUREG-0666, Appendix E, there is a graph here on recovery of off-site power. And if I want 95 percent confidence in terms of the time it says it will take, 30 hours in terms of the recovery time. That is on page E-13.

MR. BARANOWSKY: I don't think I would interpret that graph that way.

MR. LIPINSKI: Do you want to give me your version?

MR. BARANOWSKY: I think you have a probability plo there, and if you want to have confidence what you need to know is what is the uncertainty band about that line. And you will find that you can have 95 percent confidence that off-site power can be restored in say one hour with much less, or a much different probability than 95 percent confidence that

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

all losses of off-site power will be restored in whatever it is, 30 hours, there.

We don't have confidence bands around that particular--

MR. LIPINSKI: How do you interpret the 95 percent specification that goes on the 30 hour time interval?

MR. BARANOWSKY: That says that 95 percent of all off-site power outages will be restored within 30 hours.

MR. EDISON: That's not a confidence limit. That's a point estimate.

MR. BARANOWSKY: I'm sorry, maybe I used the wrong words, but it depends on what we want to take for a specification on recovery. If we want to cover 95 percent of all the cases, then we should assume that the plant is going to be out for 30 hours, if that's what we want to do.

MR. LIPINSKI: Where else would you drop the probability? Only cover 10 percent of the cases, and say we're going to be -- this doesn't even go down to 10 percent.

MR. EDISON: If you drop down to 2 hours, you will see it's still 70 percent.

na

s

MR. LIPINSKI: Well, at a tenth of an hour, which is six minutes, that is 25 percent.

MR. BARANOWSKY: The point is that would be one factor that goes into your probability in terms of estimating the likelihood of an outage of AC power. It is like the diesel probability. Maybe on the average they fail at 10^{-2}. With 95 percent confidence on the bill, it might get 10×5^{-2}. And if we did 95 percent confidence limits on all probabilistic estimates, you would end up with all the upper bounds and you would see some significant numbers.

I am not saying that is correct or incorrect, but we do our estimates based on the median values and just recognize that there is an uncertainty involved. Generally most of our evaluations are based on median estimates in comparison to other things.

MR. EDISON: Can I point out that this particular input, this recovery time is one of the factors we are studying in the Task Action Plan A-44 that is getting under way now. We expect this curve to change and add much more data.

MR. LIPINSKI: When you pick the median data, half your plants would be successful if that is where the spectra were selected. The ones that are above that limit are not going to be very successful. If I look at the two-hour outage time in this particular case, that is 70 percent. Fifty percent is a half-hour on this curve. If you pick a two-hour time interval, it says 70 percent of the plants are covered, the other 30 percent are not.

MR. EDISON: Yes. It says if you lose off-site power, the chances are only 30 percent that we will not recover it within two hours.

MR. LIPINSKI: Then you factor that into the probability of core melt.

MR. EDISON: That is correct.

MR. ROSA: If I may interject, that is for off-site power only.

MR. LIPINSKI: Yes.

MR. ROSA: We do have the backup on-site system.

MR. EDISON: Of course there would be a recovery factor of some kind applied to the on-site power system, to the diesels or whatever the system is.

MR. RAY: Any other questions?

(No response.)

MR. RAY: Thank you, Mr. Baranowsky, Mr. Edison.

We are entering now into our last topic of the day, which is a discussion by Dr. Bickel of a report on the analysis of LERs relating to electrical system malfunctions.

MR. KERR: You wouldn't consider a short break, would you, Mr. Chairman?

MR. RAY: At the suggestion of Dr. Kerr, I will be glad to have a short break. We will wait until 3 o'clock.

(Recess.)

MR. BICKEL: My name is John Bickel. I am a former ACRS fellow. I would like to summarize a report which was written at the request of the ACRS members.

MR. KERR: Incidentally, we are willing to forgive you for your past sins.

(Laughter.)

MR. BICKEL: Okay.

The study I will be talking about was an analysis of about three years worth of LERs related to malfunctions in the on-site electric system at nuclear power plants. The study was undertaken in response to a letter by Mr. Epler of July 1979.

In reviewing the history of it, I found that there were basically three concerns stated. The first one was that as reserve generation would diminish or get smaller, should you anticipate more frequent interactions between the grid and the plant, some of which would undoubtedly be very severe?

(Slide)

During some of these transients, can protective features intervene in the operation of the on-site electric system in an unanticipated manner and make the transient a whole lot worse? There was reference to the Goldberg cascades.

And three, have there been complex protective features incorporated in some of these plants that are unusually complex such that during test and maintenance you found yourself in rather unusual modes if you were subject to a transient?

The recommendation in that letter was that an examination be undertaken of the whole on-site electric system to try and find if there were any problems that we should be concerned about.

(Slide)

The ACRS recommended, therefore, that a systematic review of actual operating experience with existing plants be undertaken with three purposes: identify the specific failure modes that were observed and the consequences; highlight any unusually severe sequences; and try and identify areas which would seem to need improvement just based on you see the thing happening again and again and again and nothing seems to be done about it.

(Slide)

To carry out this study, the following scope was proposed. Include the examination of electrical system LERs for a three-year period. We chose the time period 1976 through 1978, inclusive. We took this request, had Oak

Ridge generate a computer printout of all their catalogued LERs related to the on-site electric system. They provided us without about 1177 LER summaries.

Using these, we attempted to identify the specific failure modes and consequences. We highlighted some of the ones which we felt were quite severe. Additionally, we would also take a side look at NPRDS on any events that seemed to be happening that seemed like they were fairly infrequent. We need a little wider range of data.

Another thing we wanted to do was find were there any glaring inconsistencies with WASH-1400 data. I don't mean we were going to sit down and, using every LER we had, attempt to calculate a certain, you know, probability of failure of a device. What I wanted to do was sit there and say did WASH-1400 say this is a highly unlikely event, but if you looked at it in actual experience you found that the thing was really not so rare, that something was going on all the time and it was somehow missed. So we wanted to perform that check additionally.

And again, we were going to look at areas where we could improve the thing.

(Slide)

Initially I considered when we started the project out if it would be possible to develop a generic or simplified model of the on-site electric system such that we could lead to a simple fault tree that we could then look at the events that occurred and then try to follow them on a roadmap using a simplified fault tree. We could then identify sequence probabilities to just do some cross-checking.

When we started looking, there were a lot of various differences among the different designs. There were different levels of redundancies in circuits in the way they are interfaced. There are many different schemes for accomplishing the actual interface between the actual off-site circuits and the on-site electric system.

The other thing we noticed -- I see a major typo here. It is interconnections. There were many different ways that we found of the interconnections for control power. In other words, some of them had an alternate source for control power for some of the main breakers. They were just not similar enough that I felt that you could use a single fault tree model, no matter how much you simplified it, and then have it relate to something.

What we did choose to do was to look at key functions that had to be achieved if you wanted to prevent core melt. That would be: you have got to get reactivity control, inventory control, control pressure, get heat out of the core and remove it to an ultimate heat sink. So we don't care how the plant and the grid interact with each other. As long as you do these things, you are okay.

It is somewhat simplified because for the most part on disruption of AC power, or even DC power within the plant, you are generally guaranteed that you are going to scram. I am sure somebody will say, well, there's that one in a thousand chance that you could find some bizarre ATWS event or something. But we just wanted to eliminate that, so we were going to concentrate on achieving emergency AC power for essentially the last four items: inventory, pressure, heat removal and heat sinking.

(Slide)

To do that we had to separate out all the LERs. We chose a breakdown of kind of eleven layers. The levels of redundancy in these functions or system areas differs, of course, from plant to plant. We broke it down into off-site circuits and startup transformers as one block; the automatic load transfer function -- you know, when the generator trips you switch over to the startup transformers; load shedding devices, devices that are going to disconnect big loads if you start to get a degraded voltage situation.

ESF loss of normal power logic. That's the stuff that tells diesel you better get going and controls that function. The air starters we separated out from the diesel generators because after a preliminary review of the LERs, we uncovered the fact that about one-fifth of all diesel generators, at least related to LERs, seemed to be originating from failures in the air starting systems, and I will get into that a little bit later.

Diesel generators, the load sequencer, the battery chargers, station batteries, the inverters or MG sets, and last of all, fusing and protective relaying.

(Slide)

In other words, if you take a look at this, one could envision for a simplified plant, which is just to give an example, a train of power coming from the outside world down to some vital ESF system on the bottom.

The points I would make are that we know that there were a lot of differences with the number of battery chargers used, the way the batteries were rigged together, and the number of breakers that were found in the DC switchboards and that type of things. There were a number of differences.

(Slide)

We started the thing out in the fall of '79. We acquired the LERs. We categorized the LERs into which key system. By the term "key system," I would use the term of the breakdown into one of eleven types of malfunctions: if it was with the diesel, if it was with the load sequencer or whatnot. We attempted to break them down into one of those categories only.

We prepared checklists such that we could see what was the primary thing that failed and what other things seemed to be tied with it, and the checklist was one way of just going through systematically all the LERs. Certain LERs were eliminated as trivial. I want to emphasize that because if you are going to do statistics, you have to look at the whole darn thing. So we threw out LERs that related to minor things fuse failures in the power supply and nothing happened.

We were interested in events that prevented you from achieving core cooling, that type of thing. In other words, if you had a fuse fail in a power supply to an environmental radiation monitoring system, that was not really part of what we were interested in in this study. It might give you some indication as to how reliable fuses were for small power supplies, but that is not what we were interested in in this study.

We looked for simple trends. In other words, did you notice that if you had, say, a failure of a battery charger, what did this lead to? How did you observe it? Was it caused because you got an alarm or did it lead to a major transient and that is what led to the guy going back and saying we have had this transient because we lost our battery charge or something.

We looked at these trends, tried to get as many as we could, and I would acknowledge that there are undoubedly some trends which you are going to miss if you have a study with a large number of LERs. They are hidden for a whole number of reasons. The LERs are written different by different utilities. Some of the utilities will actually report the make and model number of some major components that fail. Others just say, you know, this unit tripped. So there is a possibility that some trends could occur that we did not pick up.

We made comparisons to the WASH-1400 data base and a few other. I also looked at the IEEE 500 reliability data, and we tried to see if things like inverter failures, which there appeared to be a lot of them, were occurring at a higher frequency than one might anticipate.

We pulled out four or five events that we viewed as significant. They, of course, were also singled out by everybody involved. They highlighted major places where you might want to rethink about certain areas about emergency power. Then we categorized the things that appeared by like potential fixes.

(Slide)

The major findings that came out of this are put into a series of tables. There is another typo I want to go over. Well, there are a bunch of typos in these. It is a draft report, I guess.

We came to the conclusion that if one looked at things like loss of off-site circuits as being a disrupting event, I pretty much think I would say that it really makes me wonder what you are gaining out of trying to add things like a lot of redundant off-site circuits and modifications of that nature.

A lot of the ones for the three-year test period we saw, a fairly hefty number, were all related to things that an operator has absolutely no control over, nor does the utility. We found things like ice storms knocking out Pilgrim on a rather frequent basis. Consumer Power Midland had a lot of loss of off-site power events. Forest fire creating a big cloud of smoke that went through a switchyard and arc'd everything. Arkansas Unit 1 tripped a couple of times in tornadoes. It appears there are a lot of tornadoes in Arkansas.

When we looked at the number of things that were related to things like environmental effects versus things that were related to something like switching errors where the operator just did something really stupid, there was a fairly appreciable number that were due to environmental effects.

It leads me, at least, to a conclusion that in trying to improve the reliability of the off-site circuits, you might be spending a lot of money and it is kind of questionable what you are going to achieve from it. I got the impression that additional service was clearly not cost-effective because you couldn't do anything about natural phenomena.

We looked at other bizarre events affecting the outside world, like system undervoltage. They were clearly very rare. System underfrequency were equally quite rare. There are some things I guess I might view as remedial that one might do. A lot of the undervoltage stuff came about as a result of the Millstone event, which I guess was mentioned this morning.

Under frequency you can look at what happens. It generally appears that the regulatory criteria is sufficient conservative. Usually the generator trips the plant out. The reactor protection system will see some type of an effect. We found failures of auxiliary and startup transformers were essentially quite rare. They are basically, as one might expect, fairly high reliability devices.

What came up as being useful would be a review of the susceptibility of passing high voltage in the low voltage systems, and that was pointed out by the -- there was a severe event at Beaver Valley, I guess. There was a flap about that a few years ago, whether high voltage could pass from the high voltage side to the lower voltage side and affect large strings of equipment.

(Slide)

Continuing on through the other systems, switchyard breakers. The failure probabilities given in WASH-1400 appear to be right, very close to what you would expect. If you took those failure rates and multiplied by the number of plants, the anticipated number of breakers, you came up with roughly about the right number of LERs.

Of course, that doesn't say that that proves the numbers; it just says that it doesn't look like there is a glaring inconsistency. I get the impression when you look at it that it doesn't appear you are going to get a whole lot of improvement from improving the design of breakers. You know, a breaker is a breaker. You could spend a million dollars and I doubt you are going to make a hundred-fold improvement in how reliable they are to even open or close.

The load shedding logic failures were very rare. One of the areas I think we did see in there, there were some set point drifts I think we noted in there in a few places, and it didn't appear that there was a whole lot you could do to the system because it was already a fairly reliable system.

The diesel generators and the air starters was an area, as one might expect, that accounted for about half of all the LERs related to the on-site electrical systems.

One of the things we looked at was, if you separated out the problems with the air starters, it comes to about one-fifth of them. The main problems I think we saw when we looked at them was leaking in the air system, leaks of the air. It would be continuously bleeding air out and continuously cycling the charging, plugging of the airlines.

One of the ones we saw was dessicate crystals for drying the air somehow managed to plug up a small air relief valve and kept it continually open. It was a fairly large number of those types of malfunctions.

The NUREG put out on diesel generator reliability -- I believe it was NUREG-0660 -- highlighted a number of ideas which they thought might work, and I listed those. Addition of air driers for removing condensation. A number of the LERs we found had indicated that there was a lot of buildup of rust, gunk and crud because the air inside kind of the holding chamber that you are going to use to give a blast of air to start the diesel -- there was rust and there was a lot of water. And sometimes, I guess, when you got the water at the bottom, it would hit things when you opened up and tried to start. If you added air driers, you might remove some of the condensation.

They also recommended increased surveillance to detect moisture, foreign matter like buildup of rust or other miscellaneous things.

They also recommended improved air leak detection capability. This would be useful. One of the plants we noticed had a lot of problems with the diesels was Zion. They had a series of things where they had air lines leaking and it was just a matter that there was not enough directability to monitor the thing, apparently.

The diesel generators. Again drawing some of the conclusions from that other report, they recommended the provision of dust-free enclosures and improved contacts to improve reliability of electrical contact being made. One of the problems they cited was the diesel generator vaults tended to be kind of dusty, dirty areas that do not get frequent cleaning. It is not a dust-free environment. If you could keep some of this junk off of the areas that needed good electrical contact, it would appear that it might help it.

The next largest source after the air starters were tied to things that were done wrong in maintenance and test procedures in that report. Some of the more startling ones I do recall were about the diesels.

There was an LER from Zion where they had a plant trip. HPSI actuation turned on a diesel and one of the diesels wouldn't start. When they opened it up, they found that a workman had been worried about junk in the oil line, and he fashioned his own filter out of a piece of cloth, and he successfully plugged the oil line to the diesel.

We found things where workmen tried to clean a floor at DC Cook somewhere near the control cabinets for the diesel using a high pressure water hose. He just turned on the hose and the unit was apparently just dripping with water and he got more of a blast of water than he had anticipated.

For the types of things we saw in that area, you couldn't put all the maintenance errors under just one heading. It was an amalgamation of everything envisionable. It became apparent that you could use some amount of improved maintenance and tests and operating procedures. These are not the types of things that are amenable to a hardware fix.

You know, people have talked about it would be nice if you could cure the thing with hardware. For some of the things that are indicated, there are some things you can't fix with hardware. They are going to take some stiffening up of the way people work and service on them.

(Slide)

The last table here looked at -- continuing on, I guess, through that chain -- load sequencers. We found a number of events that were the result of incorrect sequence or timing. It was quite a rare event.

We also found a rare event of latch-up of a timer where, a set of time delay relays just stuck, therefore the ESF systems had to be loaded onto the diesel manually. I gather, by looking at it, I have a strong feeling that putting in a hardware modification to fix these types of things is going to be difficult.

There are a lot of these devices that are fairly high-reliability devices, and if they fail, trying to have a second hardware device, I really question if it would be the best way to go. I think it would appear, at least in my opinion, the procedures to cope with it -- in other words, identifying that you have not successfully loaded, or that you have overloaded and you have just tripped the diesel would be more appropriate.

Battery charger trips. The frequency was -- is enough that there was a fair number, like maybe two dozen in the three-year period, of battery charger trips. The one thing we noticed was that there were no consequences. In the three-year period, out of all the battery charger trips, there were no plant trips. In every single one of them, the enunciation of the failure of the unit by many different methods eventually led to action being taken by the operator in far sufficient time to prevent tripping.

The only area we saw was that some of the procedures-- one of the things -- I don't know if you would really call it a "safety concern," but the load discharge tests that were run infrequently, I got the impression that the people doing it were not very familiar with how the test was done.

There was a very large number of those types of things during the performing of the test where the unit was tripped on overcurrent. The reason was they all cited the fact that the charging current had been turned up real high to try and recharge the battery quickly. That is a procedural thing.

Station battery low voltage. Very rarely did you get a low voltage. The most common thing was problems in reading a sufficient specific gravity of the pilot cells. There are a number of plants where the thing occurs every time they test it. We found about a third of all the LERs in that area were from one plant. It kind of made me thing about a remark I heard this morning, that maybe they ought to be rethinking the way we are declaring the batteries as being dead, or in trouble.

Loss of DC distribution panel. The event was quite rare. It has occurred. I think we had two events where we found something of that nature had occurred. In both cases,

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

they were human-related during tests. One of them I believe was at a -- at Duane Arnold. It seemed to occur during shutdown where people are running around checking things.

The problem I think with the DC panel is that it is a support system. You are using DC power to control a large number of devices throughout the plant. When you disrupt it, you correspondingly disrupt a lot of stuff, and that makes the consequences tend to be unpredictable. You've got to look at it purely on a plant-by-plant basis.

I don't see how you can say just doing it here will do all of these things (indicating). It is clearly a plant by plant effect.

The more common one was not the entire loss of all the DC bus, but they tended to be in a local area.

The inverter malfunctions was, I think, one of the items that came out staring me in the face: That some more thought has to go into it. We found about two dozen inverter malfunctions. The more interesting fact was that almost each and every one of them led to very severe transients.

The cause was -- it's kind of a peculiar situation. It kind of was related to the fact that you have tied some control-related systems to a safety system that is being powered by an inverter. When you lost the inverter, all the control systems were all simultaneously led with erroneous demand signals.

Now some specific examples: Crystal River has had a fairly appreciable number of the inverters failing. In other words, it appeared that like out of about the two dozen, about six or seven were related to Crystal River, and about half of those led to some pretty severe feedwater transients.

There also had been a couple in Westinghouse plants. The usual cause was failure of an inverter in an RPS channel that just happened to be feeding the pressurizer level of the feedwater system with the control -- you know, some inputs from the control systems. When the inverter went, you lost one of the RPS channels, and you got a partial trip of one channel.

The control systems all took off in an erroneous fashion. I think the only thing that would cure the inverter situation, I seriously doubt you are going to be able to spend a lot of money to come up with a brand-new design of an inverter that doesn't trip so often. An inverter is a fairly complicated device. It is manufacturing AC out of a DC source.

The thing I think that might be useful would be to have the individual plants aware of what is going to occur if that inverter does go, and have well thought out what they should be anticipating to happen, and how quickly it could be detected.

It was apparent that in reading some of the LERs that there was not a whole lot of plans, or even what I guess you

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

would call we'l thought-out goals in the way people chose what AC loads to put on what inverter. In other words, you would have a situation like in Crystal River where the A channel inverter is the inverter you do not want to fail, because it turns out that the majority of the signals going to the integrated control system from the RPS all originat from channel A. If you lose the A channel inverter, you get a loss of feedwater.

As a result of the B / FMEA study I guess they did a few years ago, there is some movement in that area to try and upgrade the flow signal and make it a more reliable source of information.

Fusing and protective relaying. We found, again, things that I guess I would view as more procedural, and things that might help in the future. We found areas that I guess could only be classified as "insufficient fusing."

What it involved was places that had to be regularly tested that did not have test jacks, and did not have any type of, say, a small instrument fuse on it such that if you took a multimeter and put it to read "current," when you really wanted to read "volt," that happens in a number of places. And if one looks at it and says: Why the fix to that is probably not that bad. The situation was that you have a bus or a thing of control logic that you were trying to periodically test. And I think I can envision a guy with a very large set of alligator clips trying to hook the thing up with a multimeter and shorting the thing out on the bus on the control circuit.

The fix to that seemed to me to be very simple: You have to have a dedicated jack, and you probably want to put a very small instrument fuse such that if you did create that accidental short, it's not going to trip out the supply to a control system.

Another area we did see is "incorrect fusing and set points." This again is an area I don't think you're going to fix with hardware. We found instances where the -- I guess it's a common practice; I was not really aware of it. I'm not an operations type person -- was it was quite common to remove the bus fuses when you go to service a large piece of instrument, a large AC device. One would then use their absence as being a protection against somebody in the control room, even though a breaker is tagged out, going over and throwing a breaker and zapping you.

In a number of instances, the fuses were left out. One would say: Well, yes, but usually when you perform maintenance you go back and periodically you're going to go back and immediately check and do a continuity check by throwing the switch and seeing that you get the action.

A number of LERs indicated that the fuse holders were damaged or bent out of shape such that there was not a good electrical contact being made. This occurred on two

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

plants. I think St. Lucie was one of them, where they had been doing frequent work on a containment ventilating fan, and they had had a couple of LERs where they'd forgotten the fuse, and then they had a couple more where they had replaced the fuse but had bent the fuse-holder and they didn't get good electrical contact. It was kind of "ify" when they threw the switch. The motor kind of would start, but it really didn't start that well.

That item would make one think that it would be a good idea maybe to have an alternate way of blocking power to devices, rather than just having to pull the fuses. That was kind of the overview of the things we went through.

(Slide.)

Going back to what was originally asked: Are plant grid interactions going to be more anticipated? I would say in theory, "yes." However, from some small checks we did, reserve margins appear that you don't have a problem, at least for now.

The other item is that I think the provision of power to vital safety functions like your ESF systems, I think the place where one should want to concentrate on is the reliability of the on-site equipment. That is one area where the operator and the utility has a lot of control over. The reliability of the off-site grid can be viewed, I would say, maybe as an enhancement to the reliability of what you have on the on-site system, rather than vice versa.

I think for a good bit of time the people have been saying: Well, the diesels are backing up the off-site power. It is true. It's just that you can control how well your maintenance and your activities on the diesels and everything goes, and you can't do anything about mother nature.

(Slide.)

The second item: During certain transients, can protective features intervene in an unanticipated manner to make the transient worse? In theory, and based on practical and actual experience, yes.

Apparently the most frequent case where this occurred was in a situation of incorrect protective set points. A good example was incorrect load shedding. In other words, you tripped off a load before you really actually had to, because the set points had been put in incorrectly.

Excessive load sequencing: If you had the diesel generator, you tried to put on too much onto it too quickly, you're going to trip the diesel and take the whole thing down, and the guy is going to have to do it manually.

So it is clear that certain protective features can cause you a problem.

(Slide.)

The third item: Have certain complex protective features yielded unusual plant operating modes while in test and maintenance? Based on operating, actual operating experience, the answer is again "yes."

The most common place where I think this type of thing appears is on protective interlocks and breakers. There are an awful lot of them. The control wiring for the breakers is usually fairly complex, and in a lot of cases the operators in the plant are not specifically aware of all the interlocks that exist. They have procedures to allow them to work around the thing.

There were instances where operators performing operations with the breakers got themselves into a state that they couldn't get out of, because they didn't know the wiring that was controlling the breakers and the interlocks they had. Their only alternative was to literally disconnect themselves.

There were two events -- one at Davis-Besse -- where they essentially got down to that. In another case, it was an event I guess at Indian Point where they found themselves in a position where they were interlocked out from doing what they wanted to do, and their only solution was to essentially create a loss-of-offsite power to start the diesels.

And this, I guess, summarizes the result of the study, or the study of the LERS, and I will try to answer your questions to the best of my ability.

MR. EBERSOLE: John, I was interested in the absence of valves. I look at valves as being about half electrical

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

and half mechanical apparatus, and there are an awful lot of them, and I don't see anything in here about them in any electrical context. Why was that?

MR. BICKEL: We were studying the mode of delivering power to the devices, not the functioning of the device itself.

MR. EBERSOLE: So that is why we don't see that?

MR. BICKEL: That's why you don't see valves. The search that was done that produced this list of about 1107-something LERs was keyed on -- I think the key word was "on-site electric system" or something of that nature, in diesels, loss of off-site power.

We did a search that merged the common denominator of all of those, and we did not look at valves' electronic control systems. We basically looked at the sources of power for those devices.

MR. EBERSOLE: Okay.

MR. EPLER: John, I have a question that may sound like a speech, but then how else can an ACRS consultant make a speech?

(Laughter.)

MR. EPLER: This is a rather complicated question. 35 years ago in designing the first control system for the first light-water reactor, we discovered that the rod drive motors were polyphase. Now polyphase motors are just beautiful. Most of the time they'll do what you want better than anything

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

else. But sometimes, they act peculiarly. Like, for example, if you blow a fuse while you're withdrawing all rods, and you suddenly want to reverse those rods, they won't reverse. They just keep coming out the same way. This is embarrassing.

Someone outside the plant can reverse two wires and all your rod drives will run backward. This is embarrassing. Now it's only "embarrassing" because our systems could cope with that. We said, "It's bad engineering."

So from then on, all the plants they've built after that, all critical motors were single phase so their failures would occur randomly and not across the board.

I discovered a few years ago an LER in which, unbelievably, polyphased motors were opening and shutting valves. Someone reversed the phased sequence on a bus and all the valves that were supposed to close opened; and all the valves that were supposed to open, closed. I said, "My god! This is terrible."

Are these valves important? Nobody seemed to know. I kept asking people: Do we still have valves on polyphased motors? I don't know.

Well, then I got to thinking about it. Look, suppose someday your diesel is down, and when you put it back together you check it our for phase rotation and discover, sure enough, the phase rotation is backward.

So the front office sends a crew out on my next shift

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

to correct this.

Now at Cooper, a year or so ago, we had a situation where a service water pump was down and disassembled, and the front office sent a crew down to align the coupling, to align the set and disconnect the coupling. They did, but on the wrong unit.

So I propose that when you send a crew out to reverse the phase on this diesel, they may do it on the wrong diesel. Now you've got two diesels with the phase reversed. So then you have these possibilities, and they're delightful.

MR. BICKEL: I would agree, but the only thing is, if you come up with the hardware --

MR. EPLER: Well, you're spoiling my story, because I'm not through, yet.

MR. BICKEL: Okay.

MR. EPLER: You have these delightful possibilities.

Suppose that you test the diesel. You have two possibilities. You test it by synchronizing. And if you synchronize the thing with the phase rotation backward, it much worse than a short-circuit. You may wreck some equipment.

The other possibility is that you assume load without synchronizing, but the motors all run backward and begin to destroy some functions, and maybe cause a scram. Now you're in poor shape with the scram with your phase rotation backward.

Then there's another possibility, that you don't discover that the phase rotation is backward on two diesels, and you get a loss of off-site power, and all the valves in the plant that are supposed to open, close; and all those that are supposed to close, open. And these are demanded to perform on the basis of protection systems that cause these valves to go, and you can't do anything about it.

Now the limit switches are in the wrong direction, so the valves continue to spin, and spin, and spin, and tear themselves up.

Now tell me this can't happen? Nobody ever could. Tell me this can't happen.

MR. BICKEL: I don't know. I would say the limit switches would probably shut you down.

MR. EPLER: No, they're in the wrong direction.

MR. BICKEL: Yes, but they've got a full-open, and a full-close.

MR. EPLER: But if you turn it to full-open --

MR. BICKEL: Are you trying to tell me that you're going to miss both of them, somehow?

MR. EPLER: -- the wrong limit switch, it won't do anything. It won't work.

MR. BICKEL: Okay, okay, you've got a point. They're on the wrong end of the travel.

MR. KERR: Well, if you follow the scenario proposed by Mr. Epler, you can't say it can't happen.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. BICKEL: I've learned that.

MR. EPLER: Well, is anybody worried about this? Or are they just going to wait until it happens?

MR. BICKEL: I would first of all point out that I really did not consider that type of sequence.

MR. EPLER: Well, you gave us a clue. You gave us a clue.

MR. BICKEL: Yes, I agree.

MR. EPLER: You said that it's been assumed that a complete loss of power was the worst thing that could happen. But then you told us that a degraded frequency or a degraded motor would be bad, too. Now I say that phase reversal could be even worse.

MR. BICKEL: The main point we were attempting to do with the study -- I'm not trying to dodge the question anymore than I am -- was to review LERs to determine what, if anything, we could possibly glean from operating experience.

MR. EPLER: Well, I started off with a LER.

MR. BICKEL: I agree. Thank God it was not in the three years that I was looking at it.

(Laughter.)

MR. BICKEL: Obviously, you know, you're going to get to some event that the only thing that is going to keep you is the smarts of the people fixing and maintaining the equipment. I am certain -- I am positive that you could find

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

other sequences --

MR. EPLER: Well, could I --

MR. BICKEL: -- put them the same way.

MR. EPLER: -- finish the question? I would say, shouldn't we ask somebody to look into it and see if this is real?

MR. BICKEL: I think one could look into it. The only question one might raise, though, is suppose we do take some person and have them look into it for six months. Is that the best application of our resources?

I guess I am not convinced it really is. I think that there are enough things in what we found just from looking at LERs that might merit a quick look right now.

One that I think that has really impressed me as underrated is the business with the inverters going. They create an immediate transient. A failure of one DC bus initiates a transient and starts you off. Failure of the ESF systems or the load shedding equipment initiates the transient and cuts you off from off-site power about the same time.

These type of things, you know, just from an observational thing, appear to be a little bit -- one of the things I guess I would want to be concerned about. They are right up there. The ability of the guy -- I'm not going to deny the guy can do it. The main function of every time -- most written procedures I've seen for operations when you do a

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

maintenance effort, the first thing you do after you think you've finished servicing the pump, or the diesel breakers, or all this sort of stuff, is to try them out and see that you really have restored them to their operating condition.

I don't think it would be that hard to run a very simple test, turn the power on and see if the valve is swinging open or closed. It's the type of thing that could be looked at very quickly, and indeed some procedures that I've seen require tests like that with a guy sitting with a walkie-talkier, or a head-phone set.

MR. EDISON: Can I offer a thought, Mr. Epler?

MR. BICKEL: Please do.

MR. EDISON: I am sure you are aware that in the BWRs there are a couple of systems that can put water in the reactor that have DC-powered valves -- the RECSI and the HPSI, with the exception of one valve inside the containment. And in the PWRs, there is an auxiliary feedwater train required on all the plants that is supposed to be AC independent. So that there is a means of at least removing heat from the reactor for some undetermined length of time until you can figure out what happened. It's not a total down-the-tubes loss.

But your suggestion of how to look into it, I would think, one, we might at least ask the human factors people what the possibilities are of going to the wrong diesel, and then doing something backwards, or something like that. That

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

might be -- and we do have capabilities in NRC now to look at human factors' problems both in NRR and in NRES. So that offers a possibility.

MR. ROSA: I would like to add something, also. The technical specifications preclude maintenance operations on more than one redundant power source at the same time. And following any kind of maintenance operation, then the diesel has to be fully tested by performance of the periodic test, which is a start-and-load-and-run for one hour.

Now it is possible that the reconnection performed after maintenance operations would have reversed the sequence. However, the test certainly would reveal this, possibly to the destruction of the diesel, but nevertheless I don't think there is a possibility that it could happen on both diesels -- that's phase reversal -- at the same time.

MR. EPLER: Well, I was struck by when you propose a sequence as an example, then someone proposes that you can fix the example. But we still have the problem. We still have polyphased motors that can run backwards, and it might not just be diesel; it might be somebody else who did it.

So I submit that polyphased motors on valves can be real tricky, and they ought to be worried about.

MR. EBERSOLE: I don't hear of too many cases like this, Ep, but I'm pretty much interested in it. What are the mechanisms that we have now that prevent this sort of thing?

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

I never have heard of any exposition of this. Certainly you check rotation of the equipment. I guess the limit switches on valves are a part of the test procedure.

So many of these operations occur, it would seem that this kind of thing would occur more often than it has.

MR. EPLER: Well, it occurs in industry. It occurs rather frequently, but with small consequences.

MR. EBERSOLE: Did you find any anywhere, John?

MR. BICKEL: I'm sitting here, and in the back of my head I'm starting to think of something. Some of the torque-- I guess the problem is, a lot of the torque switches are pulling a lot of the motor-operated valves.

MR. EBERSOLE: They are multiuniversal. They torque to close, and they torque to open. There would be all sorts of trouble.

MR. BICKEL: I'm trying to think. There are -- apparently there are several protective devices within the motor-operated valves. There is a torque. I just don't know. I don't think it goes in the right way, though. You're right.

MR. EBERSOLE: I think I have heard of some centrifical pumps that have run backwards for a long period of time, and nobody knew the difference.

MR. BICKEL: I thought it was a main feed pump. The checkvalves wouldn't allow you to do it for very long. You couldn't drain the steam generator.

MR. EBERSOLE: No, no, no. When you reverse the centrifical pump, depending on the impellar design, it might or might not create a big difference.

MR. BICKEL: That's right. That's right.

MR. EBERSOLE: It would still pump, but not as well.

MR. BAXTER: Mr. Chairman, may I interject a thought, please, on this subject?

MR. RAY: Yes, sir.

MR. BAXTER: Earl Baxter, Yankee Atomic.

Following up on what Faust Rosa said, that after a major maintenance of the DC generator you would be required to put it through a test, a loading test, and run it up for an hour or so. If you attempted to do this with reversed phase, it would not be possible to synchronize under that mode, and that would be the point at which you would detect the error.

MR. EBERSOLE: With gusto.

MR. KERR: Does the test always include synchronization?

MR. BAXTER: I can't say, offhand; but for something major, I would think it might require a period of synchronizing and loading. That is something we can check out.

MR. ROSA: I can check that out. The technical specifications require that the same test that is performed periodically on diesels be performed after major maintenance. To do that, you have to load to at least 50 percent. To do that, you have to connect to the bus and feed power out to the grid. So it does include synchronization.

MR. EPLER: Oh, tricky.

MR. EBERSOLE: One problem. A lot of our pumps are tested with bypass systems that never achieve full flow. For instance, the RHR low flooding, pressure flooding pumps. A lot of these have a moderate-sized bypass. And if you had malconnected the terminals in the motors, since you can't see the shaft, you don't know which way it's going anyway, it would develop a flow easily in the bypass mode if you would wrongfully interpret that it was not connected in reverse. You would only learn that when you needed it.

MR. BICKEL: Well, I would say that we specifically did not look at this. We did not see any events of this nature. The main thing I was trying to -- if I could restate it -- we were trying to find is: Where there are LERs that suggested there were some things we ought to look at with the on-site electric system.

MR. EBERSOLE: What are those pumps which are tested in the 15, 20 percent flow mode? How do you verify that it is starting the right way so it will be ready for the full-flow case when you want it?

MR. ROSA: As far as I know, there is no test made specifically for checking rotation. The rotation check that is made after a major maintenance, or during the construction

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

phase, or at the end of the construction phase, is relied on.

MR. EBERSOLE: Is there a requirement that the shaft construction be such that you can always see it?

MR. ROSA: As far as I know, there isn't.

MR. EBERSOLE: So it could be fully enclosed?

MR. ROSA: It could be fully enclosed.

MR. EBERSOLE: Then you would depend on the pumping outputs, and with the 20 percent bypass flow you wouldn't know if you could make full flow or not.

MR. ROSA: I do believe that the 18-month test that is required before full system operation would probably reveal whether you are getting full flow or not.

MR. EBERSOLE: So it would lay out for 18 months with full phase reversal on the motor?

MR. ROSA: If that is the case, yes.

MR. KERR: Mr. Rosa's earlier argument didn't convince you?

MR. EBERSOLE: No.

MR. KERR: That synchronization would reveal --

MR. EPLER: You wouldn't dare synchronize.

MR. EBERSOLE: This is a closed motor.

MR. KERR: No, but the synchronization is going to occur after you repair the diesel, according to Mr. Rosa.

MR. EBERSOLE: I'm not talking about diesels; I'm just alking about pumps.

MR. KERR: Oh, you're not talking about the sequence that Mr. Epler talked about?

MR. EBERSOLE: I'm talking about the motor, the loads.

MR. ROSA: Well, another thing, too, on safety-related pumps there is always redundancy there.

MR. EBERSOLE: Yes.

MR. ROSA: Okay, it is possible that you might have a phase reversal on a pump.

MR. EBERSOLE: You would consider it random?

MR. ROSA: Yes, I would consider it random. And phase reversal on two redundant pumps, even more unlikely.

MR. EBERSOLE: That's consistency.

(Laughter.)

MR. BICKEL: That would be all, I guess.

MR. RAY: Do the NRC representatives have any general comments on this study report?

MR. ROSA: I would like to make a few comments.

I didn't have too much time to read this, but I did skim over it. I thought it was a good job. It duplicates and confirms results found on other studies -- namely, that diesel generator studies, NUREG-0660 -- and it confirms some results that are included in WASH-1400. It also provides an independent look at this subject that I think is valuable to the Staff.

Task A-44 I think will benefit from looking at the study. I would --

MR. BICKEL: I will get the typos cleaned up, first.

MR. ROSA: I would make one other minor comment. That is, that in reading this report, when you used the term "on-site power system" or "circuit," you include the off-site circuits from the switchyard down to the safety buses. In other words, those circuits serving a nonsafety auxiliaries you sometimes refer to as "on-site power."

Just so there is no misunderstanding, the Staff, when it refers to the on-site power system, refers to only those circuits downstream of the safety buses. Everything from the safety buses out to the switchyard and the grid we consider off-site power.

MR. BICKEL: Yes. I can understand that. What I was referring to when I was saying you lost off-site circuits was that you were losing this (indicating) or this (indicating), just coming into the switchyard. And I will take note of that.

(Slide.)

One thing I don't think I did mention, there was only one area where I wrote up in the report where we found an inconsistency with the WASH-1400. That was related to the -- it was a quick-and-dirty calculation in WASH-1400 related to the likelihood of an operator throwing a switch, an electrical switch, and operating the switchyards found in the section on electric power like the PWR evaluation. It came up with a

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

rather small number for the likelihood of an operator throwing a switch that he normally would not throw when he's been trained to "leave this thing alone" during a transient.

We found several events where operators misoperated the big breakers in the switchyard. There were quite a few, as a matter of fact. They were usually events where the plant tripped and the guy was apparently trying to verify that certain breakers had in fact opened, according to the plant procedures, and go in quickly by the board. They were located through the wrong switch.

So there does appear to be a likelihood, and I think it is because -- I would say, my gut feels that a lot of the control boards in the plants, there is a great deal of congestion in some of those areas. This I think is a human factors problem, and I don't think it was fully evaluated in WASH-1400. But the numbers for the actual hardware pieces, there did not appear to be glaring inconsistencies.

In other words, the number of LERs that were not out of the ballpark. You can't use LERs to come up with proving exactly those reliability numbers, but it suggests that they are in the right range.

MR. RAY: I would like to get a reaction from the subcommittee members as to whether or not a presentation by Dr. Bickel would be desirable to the Full Committee. Remember, the Full Committee approved this study.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. KERR: Jerry, before we get to that, may I ask John a question?

MR. RAY: Sure.

MR. KERR: On page 1 of the abstract, John, in the first paragraph, there is a statement that: "... actual operating experience indicates that the probabilities for incorrect operator action and operational quality assurance failures used in WASH-1400 were less conservative than assumed."

"Assumed" by whom?

MR. BICKEL: Okay. In the --

MR. KERR: Or maybe I should ask what you meant to say by that sentence, because it wasn't clear to me.

MR. BICKEL: What I would say I meant by that statement, WASH-1400 made a number of statements about assuming what an operator would do in operating the electrical system of a plant during a transient.

I found that actual operating experience was less conservative than what was assumed -- I'm getting this all boloxed up -- it was not as good. Put it that way. The actual experience was that operators did things during transients with the electrical system that were worse than what was assumed in WASH-1400.

Additionally, there were some types of operational QA --

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. KERR: Wait. Before we get to QA, if you were rewriting it, then, would you say that in your view the operating experience indicates that the probabilities for incorrect operator action are greater than that given in WASH-1400?

MR. BICKEL: Yes. That's correct.

MR. KERR: Based on the fairly limited set of data, however.

MR. BICKEL: That's correct. It's just that I believe some were -- I remember seeing a number -- the one in particular that struck my mind was in the analysis of Surrey. They had a breaker there that if you threw it during a transient, it was going to give you a real problem.

They did an analysis of three operators. They had been trained, and the probability of each operator doing this, they came up with a net probability that somehow gave them 10^{-4} that they were going to throw this during a transient.

And if you looked at the -- I looked at the number of times it had occurred during events where there were disruptions in the off-site power, or there was a major transient like you just tripped the reactor, and the operator is doing the runaround through the control board checking to see that breakers have opened, and he's disconnected the generators, and he's coasting down and all these types of things. There were a number of cases where he went out and made the

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

transient a whole lot worse by throwing the wrong switches. It was apparent from what they had written up in the LER. They had hit the wrong switch -- they were right next to each other, or these types of things.

The numbers were inconsistent with what you would, if you just assumed that blanket number they had in WASH-1400 in that one place.

MR. KERR: Yes, but it seems to me that one should be careful about drawing conclusions about --

MR. BICKEL: Blanket numbers.

MR. KERR: -- a rather large population, I would think, used by -- you may be quite correct, but you may also be picking an aberation of some kind.

MR. BICKEL: I may be picking one limited report, right.

MR. KERR: Now on page 12 of the study, the bottom paragraph refers to "setpoint drifts in the actuation of logic", and then there is a statement: "This type of problem is generally difficult to fix permanently."

I don't understand why it's generally difficult to fix permanently.

MR. BICKEL: I base this on experience with reactor protection systems.

MR. KERR: I would agree that it frequently has not been fixed permanently.

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. BICKEL: Well, it is a problem that setpoints tend to drift and they drift in a continuous fashion, and every month or so you end up having to readjust them. If you didn't have drifting problems, in theory you would hardly ever have to touch setpoints.

MR. KERR: I would urge you to say that experience indicates that people don't fix them. I would like to see some evidence that they are difficult to fix, because I just believe that they're not all that difficult to fix, if somebody would give it some thought.

MR. BICKEL: I think what I'm saying, I guess it was a semantics problem. The point I was trying to make is that it is difficult to permanently fix the drifting of setpoints in some devices.

MR. KERR: Well, I think it is, if you use devices that have inherent drift in them. I think that's part of the problem. But that was just a remark. You didn't have any -- there wasn't any supporting evidence that people who worked real hard to fix these couldn't fix them.

MR. BICKEL: The one in question was, like I say, with the load shedding systems. I think one of the things, I guess at least the way I tried to rationalize it when I was reading it, and maybe I'm incorrect, was that you've got the device that you want to trip within a -- you want it to operate such that you don't trip needlessly these devices that are going to lead you to a plant trip, and yet you absolutely do want them within another certain range.

I think you've got a very narrow range, I think is what the problem was, and they were drifting in and out. Maybe it was environmentally related.

MR. KERR: On page 33, where you're discussing battery charger failures the impression I get is that you don't consider this to be particularly serious. It would seem to me, from what I have read of Mr. Epler's scenarios, that this could be fairly serious if you don't know it has occurred.

There isn't anywhere in the paragraph that I can get an indication that one always will know that it occurs, or all designs tell you right away that it has occurred, or something like that. The statement simply is: "The consequences of a battery charger failure ... are virtually negligible provided that the Station batteries are sufficiently charged." And I am not quite sure I know what that means.

MR. BICKEL: Okay, I'll try and elucidate that a little bit. A lot of the plants we looked at, first of all, have redundant battery chargers. There are two charging one of the DC trains.

MR. KERR: Epler can beat that.

MR. BICKEL: I know he can. I'll say it quickly and maybe I can get away with it.

There were two. It was also apparent that a fairly large number of them provide direct enunciation either in an indicator light somewhere, an enunciator window, something, a computer printout, some device that is telling the operator --

MR. KERR: These are not being run on the DC battery?

(Laughter.)

MR. BICKEL: Some of them are. The main thing, I think they have a little bit of time once it goes. They get an alarm, and then they can actually send somebody into the area where it is located to try and get it running again.

MR. KERR: I think as a minimum you should put a footnote somewhere saying that Mr. Epler probably would not agree with the substance of that paragraph.

(Laughter.)

MR. RAY: Are there any other questions on the details of the report?

MR. EDISON: I have a couple of comments, Jerry.

First of all, let me say that I think this is just excellent to be reviewing the operational data this way. I think the whole agency could do with a whole lot more of this kind of work. There are hundreds of things in this report that I agree with, and there are only two that I would like to mention that I have some comment about.

One is on page 34, down at the bottom of the page. This particular failure mode exists. I don't think this example is a very good example of the failure mode, because

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

when we are down at refueling you have one situation, and when you're up at power you have another. I think when you're up at power, the operator is not out doing that kind of instrument monitoring and certainly cannot initiate a trip when he's down at refueling.

So I agree that you --

MR. BICKEL: I agree with the comment completely.

MR. EDISON: You can go through the sequence, but I don't think that's an example.

The other comment is at the top of page 35. I have to disagree, based on today's presentation, that the effectiveness of improvements in batteries and DC power reliability can only be evaluated on a plant-by-plant basis.

We did our best to do a generic analysis. We did go to plant by plant data, and we looked at half-a-dozen plant configurations to decide what maximum dependencies were. But I do think you can do some generic evaluations, as well as plant-by-plant analyses.

MR. BICKEL: Well, I had some feelings about that. I was going to say, one of the things that hits me about the minimum -- the idea of a minimum system is, when you are examining a DC-dependent device, how many small manual disconnect type breakers are you assuming exist between the battery and the device you're trying to run?

You know, it would appear to me, the events that I guess we saw -- that I saw that were related to where you had a failure of DC power all seem to be things where an operator or somebody was doing something with one of these. Granted, at least the ones that occurred in the three-year period were very few, but the question arises that there are some tests that are done on DC buses while at full power, and there is some number of protective devices in the DC switchboards that would attempt to protect you. But they have the effect of cutting off a whole leg of the DC -- of a DC bus that might be carrying five or six devices on it.

The thing that gets me is: How would you define "minimum," you know, a minimal design for that situation? In other words, how many levels of relaying do you have between the battery and the devices?

MR. EDISON: Well, there are many ways to try and make a generic study out of a lot of plant variations.

MR. BICKEL: Right.

MR. EDISON: One might say, well, if the worst plant has six devices, I'll do an analysis with eight and make them the worst devices I can think of, and then do a generic -- or a bounty type of generic study on that basis. There are generic things we know about the systems.

MR. KERR: You could say in that sentence that on the basis of the LER study, the authors of this report are convinced that -- and then there would be no way he could

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

disagree with you.

(Laughter.)

MR. BICKEL: It's the area of human actions which is one thing that bothers me about it. That's the one area where I really just don't know how you come up with one generic one. If I saw it, maybe I could have a better feel for how I deduce it.

MR. EDISON: The other comment I would like to make is a request. Could I get a couple of extra copies of the report so that we can make them available to our contractors on the station blackout program, and try to take advantage of some of the work you've done?

MR. BICKEL: I don't see any problem with that. This thing was hurriedly typed right before Christmas, and there are some rather glaring typos in it. It is just in draft form. I don't see any reason why not.

MR. RAY: There was a related question which I would like the subcommittee's reaction to. That is, when this thing is corrected and it is no longer in draft, the proposal was to issue it as a NUREG. Do any of you have any misgivings about that? We think there may be useful information here that would be available to all those active in the industry.

MR. EDISON: What happens to it after that? Because a couple of years ago, a fellow named Michelson did some work on a pressurizer level problem. Once the report gets written

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

and published, all these identifications, what do we do with them? Does something happen now?

MR. RAY: They're available in the public document room, and they're distributed between the divisions of the Agency, I would expect. Therefore, the information is "promulgated," if you will. That is better than having this, if you will, restricted to just an internal report of one working group.

MR. EDISON: I wholeheartedly agree.

MR. KERR: If I were the authors -- maybe they've already done this -- I would circulate this among a slightly larger audience than it has had up to now and ask for comments, not because I see anything wrong with the report, but because I think it might profit from some more general comments from organizations like TVA, or Duke, that have had a good bit of experience, and perhaps from some vendor organizations -- unless this is likely to take so much time that it keeps it out of the public domain. I think it would just be helpful to have comments.

MR. BICKEL: Bill, I had the new associate of mine, the Chief Electrical Engineer at Northeast Utilities, Arnold Robee, has looked the thing over to see if he had any comments on it. He commented on certain areas of it, and I was looking at others to see -- The usual thing, when someone sees it, based on the LERs, that they can't believe some of the numbers that occur. The distribution startles most people, because they are used to their own problems. You know, that is the thing that I think they are trying out: Is it consistent with what they have seen?

But I agree. I think that would be a better way to handle it.

MR. RAY: I think that is an excellent suggestion. That distribution could well include the NRC divisions so they could crank into it and tell us what they think would be worthy of incorporation into the final product.

MR. EBERSOLE: Mr. Chairman, may I ask a question?

MR. RAY: Yes.

MR. EBERSOLE: John, you mentioned something about doing some better testing work while the system was on line at full power. If I can go back to the report on page C-12, I had a little twinge when I read Item 4 on H.P. Robinson where it says that a tech spec was violated which required the reactor to be noncritical to disable one of the two available DC power sources.

The fact that the reactor is not critical doesn't reduce the necessity for having the battery. What criteria do you now have or contemplate putting on operators to disable one of the two available DC sources? I mean, to do some heavy maintenance on it and put the plant on a single track configuration for a limited period of time when you do the

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

repair or restoration work on this other leg? Do you have a criterion for that?

MR. ROSA: The standard technical specifications I believe require that you go to cold shutdown within two hours. At the end of two hours, you start going into cold shutdown after declaring a battery or DC bus inoperable.

MR. EBERSOLE: You're not eliminating the responsibility; you're going to eliminate a big transient.

MR. ROSA: We're going to eliminate a big transient and provide additional time to take corrective actions if something happens.

MR. EBERSOLE: Two hours is your judgment? He must do it within two hours?

MR. ROSA: Once a batter or DC bus is declared inoperable, two hours. If it can't be fixed in two hours, you immediately start going to cold shutdown.

MR. RAY: Any other comments?

(No response.)

MR. RAY: May I get back to the question of whether or not you feel this is worthy of a brief presentation to the main Committee?

MR. MATHIS: Yes.

MR. KERR: I would say it certainly depends on whether John wants to make a presentation. I think the report is rather well written, and that people who will read it will get more from reading it than a presentation. But --

MR. BICKEL: It's kind of like a dictionary. Dictionaries have a lot in them, but it's really had to try and make this into an eye-catching --

MR. KERR: What do you think? Do you want to make a presentation?

MR. BICKEL: If I had my opportunity, I would like to get some more comments and get the typos cleaned up in it. I was really under a lot of -- we had a lot of trouble getting the draft typed. It was Christmas time. Everyone was off. I would like to at least get one really nice, cleaned up version of this thing out on the street, and have other people aware of it.

The business about some of the things that just came out of it were a little bit stunning to me. Like I say, the inverters, they stuck out like a sore thumb. I had never heard anybody ever complaining about inverters before.

MR. KERR: Well, I have, but his name was Bickel.

MR. BICKEL: When I was reviewing it, of course.

MR. RAY: I've heard comments by a chap named Epler, on occasions.

MR. EBERSOLE: John, when you look at it again, I would like, if you could, to have a look on characterizing the kind of loads that are put on these so-called "fail-free" buses, the inverter buses, in the context of whether they should be there, or someplace else; whether they are a switchable power source.

MR. BICKEL: The thing I wanted to point out was, the thing that was causing the problem was not the loads on them. The good case I really remember, I wrote up kind of in detail about Crystal River was that they had the 8-channel, the RPS, you know it's vital, an uninterruptable bus, or whatever you want to call it. The A channel inverter feeds a signal isolation or buffering amplifier to the flow signal, which they are tapping out of the RPS.

Now when you fail the A inverter of that RPS design, you get zero volts coming out of the RPS for the flow analogue signal, and that integrated control system that says zero flow, and it does a whole bunch of very quick actions with the controllers, and it essentially gives you what looks like a very large reduction in feedwater very quickly. And it is guaranteed. You fail that A inverter, and you get a loss of feedwater. It's direct, and you get several other things at the same time.

It was not that you had loads on the thing. It was just that, what were the things that were coming off of it?

MR. EBERSOLE: That's what I really mean. Why should this load be on this inverter?

MR. BICKEL: I don't object to the idea of the classical control protective interaction. A lot of people were

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

upset about that for years on end. What hit me, though, was something like a cross-checking to see if it is a valid signal would have cured the problem. Maybe small things like that. If there was just something to make sure that that "zero volts" was a valid signal, you wouldn't have that type of a problem.

The same thing could be done I think on some of the Westinghouse plants where they use the feedwater flow from the RPS, they use pressurizer level, and things like that. If there was additional cross-checking to make sure it was a valid signal, an inverter failure is not going to cause all those problems.

MR. EBERSOLE: What I'm getting at is: Within the time of switching cycles, not much happens in big physical systems.

MR. BICKEL: It depends on the system.

MR. EBERSOLE: Yes. But I'm saying, not much happens in these ponderous systems, hydraulic systems. Yet you will find systems put on a fail-free bus, or whatever you want to call this bus, on the apparent premise that they can't mix a 60-cycle wave. They can. And so what ought to be on there is something that really can suffer a switching transient without an upset; to get it off there and put it on some other source would, I presume, be better. It would still have the benefit of avoiding AC loss, but it need not -- unless you really need to avoid missing a few 60-cycle waves, why should it be there?

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

MR. BICKEL: Yes.

MR. RAY: Well, I sense no enthusiasm for the idea, at least at this stage, to make the presentation or ask for time at the main Committee?

MR. MATHIS: Wait a minute, Jerry. It seems to me that this is an important part of this overall subject. We basically as a committee have asked John to do this work. Now whether it's completely polished I don't think is that important.

MR. BICKEL: It could be done, yes; that's no problem.

MR. MATHIS: But the summary of it, I think, is owed to the committee.

MR. BICKEL: Yes.

MR. MATHIS: I think it should go along with the other part, because it completes a part of the story. Now maybe others don't agree with me, but that is my feeling.

MR. KERR: I was trying to find out if John wanted to make a presentation. I would be delighted to have him make one, if he wants to. If he doesn't want to, I guess I'm inclined to --

MR. RAY: Maybe I'm twisting his arm, but I've never sensed any bashfulness in John Bickel.

MR. BICKEL: My only concern is I would like to get the thing polished up before it is done. I think it could be done, but it's just got a bunch of typos in there. There are

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

a couple of sentences in there where there's a word missing, and it completely changes --

MR. EBERSOLE: But that wouldn't alter your verbal presentation.

MR. BICKEL: No, that's true. I might want to clean up some of my slides, but I could do that.

MR. RAY: Suppose I get off dead center here by suggesting that at least the summarization of the document that you now have in your hand, reproductions of the exhibits, be made available to the main committee. And I suggest to the main Committee that they provide time, schedule time in a future meeting for a presentation by Dr. Bickel along these lines. In the meanwhile, he can be cleaning up the document and possibly the scheduling will coincide with the availability of the cleaned up version of the work document.

MR. KERR: Clean up his act, you're saying?

MR. RAY: Yes.

MR. KERR: Okay.

MR. RAY: Okay. Are there any questions remaining in anyone's mind on any of the topics that were discussed today? The principals from the morning presentation have gone, but those who are responsible for management of the program are still here, if you have any flashback questions you would like to ask, because the time is still available within scheduled termination.

(NO response.)

MR. RAY: Okay. There are no questions remaining and the meeting is adjourned.

(Whereupon, at 4:28 p.m., the meeting was adjourned.)

* * *

300 7TH STREET, S.W., REPORTERS BUILDING, WASHINGTON, D.C. 20024 (202) 554-2345

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: January 22, 1981

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.

ANN RILEY

Official Reporter (Typed)

[signature]

Official Reporter (Signature)

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: January 22, 1981

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)

Include in transcript

STATION BLACKOUT

UNRESOLVED SAFETY ISSUE A-44

P. W. BARANOWSKY
NRC TASK MANAGER

DEFINITION OF ISSUE

Is the Loss of All AC Power at Nuclear Plants a Relatively High Probability Event?

Are the Risks Posed by Station Blackout Accidents Unacceptable?

TECHNICAL APPROACH

Evaluate AC Power Reliability and Cost Effective Improvements

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

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 WRSR SASA Program

Include in transcript

SUMMARY OF REPORT:

ANALYSIS OF L.E.R.s RELATED TO ELECTRICAL SYSTEM MALFUNCTIONS

PRESENTED BY: DR. J.H. BICKEL
(FORMER ACRS FELLOW)

POOR ORIGINAL

WORK UNDERTAKEN IN RESPONSES TO CONSULANT'S LETTER
FROM EPLER IN JULY 1979

CONCERNS:

1) AS RESERVE GENERATION DIMINISHES SHOULD WE ANTICIPATE MORE FREQUENT PLANT - GRID INTERACTIONS? (SOME OF WHICH WILL BE SEVERE)

2) DURING CERTAIN OF THESE TRANSIENTS, CAN PROTECTIVE FEATURES INTERVENE IN AN UNANTICIPATED MANNER TO MAKE THE TRANSIENT WORSE?

3) HAVE CERTAIN "COMPLEX" PROTECTIVE FEATURES YIELDED UNUSUAL PLANT OPERATING MODES WHILE UNDERGOING TEST AND MAINTENANCE?

EPLER'S RECOMMENDATION:

UNDERTAKE "AN EXAMINATION OF THE ENTIRE SYSTEM BY SYSTEM SPECIALISTS"

POOR ORIGINAL

ACRS RECOMMENDATION:

UNDERTAKE A SYSTEMATIC REVIEW OF ACTUAL OPERATING EXPERIENCE WITH EXISTING ONSITE ELECTRIC SYSTEMS.

- IDENTIFY SPECIFIC FAILURE MODES & CONSEQUENCES
- HIGHLIGHT UNUSUALLY SEVERE EVENT SEQUENCES
- IDENTIFY AREAS WHICH WOULD SEEM TO NEED IMPROVEMENT

POOR ORIGINAL

SCOPE OF STUDY:

- EXAMINE ELECTRICAL SYSTEM L.E.R.s FOR 3YR TEST PERIOD
- IDENTIFY SPECIFIC FAILURE MODES & CONSEQUENCES
- HIGHLIGHT UNUSUALLY SEVERE SEQUENCES
- EXAMINE N.P.R.D.S. SUMMARY FOR RELIABILITY DATA
- CHECK FOR GLARING INCONSISTENCIES WITH WASH-1400 DATA
- IDENTIFY POSSIBLE AREAS FOR IMPROVEMENT

POOR ORIGINAL

INITIALLY WE CONSIDER DEVELOPMENT OF A SIMPLIFIED (GENERIC) ONSITE ELECTRIC SYSTEM FAULT TREE MODEL.

- THIS WOULD HAVE ALLOWED COMPARISON OF ANTICIPATED vs. ACTUAL FAILURE RATES OF KEY SYSTEMS

- COULD IDENTIFY SEQUENCE PROBABILITIES

HOWEVER THIS APPROACH WAS DISCARDED BECAUSE:

- NON-TRIVIAL DIFFERENCES EXIST IN ELECTRICAL SYSTEM DESIGNS FROM PLANT TO PLANT

- DIFFERENT LEVELS OF REDUNDANCIES EXIST

- DIFFERENT SCHEMES ARE USED FOR PLANT-GRID INTERFACE

- DIFFERENT INTERCINNECTIONS EXIST FOR CONTROL POWER

POOR ORIGINAL

CENTERES ON KEY FUNCTIONS AND HOW ELECTRIC POWER EFFECTS THESE KEY FUNCTIONS:

- REACTIVITY CONTROL (REACTOR SHUTDOWN)
- COOLANT INVENTORY CONTROL
- COOLANT PRESSURE CONTROL
- REMOVAL OF HEAT FROM CORE
- ULTIMATE HEAT SINK

NOTE:

- ON DISRUPTION OF POWER: REACTIVITY CONTROL ACHIEVED VIA SCRAM
- OTHER ITEMS DEPEND ON AVAILABILITY OF EMERGENCY AC/DC POWER

THUS:

CONCENTRATE ON ACHIEVING EMERGENCY AC/DC POWER

POOR ORIGINAL

ANALYSIS OF ACHIEVING EMERGENCY AC/DC POWER

ONSITE ELECTRICAL SYSTEM WAS BROKEN DOWN INTO A CHAIN OF ELEVEN KEY SYSTEMS WHICH FUNCTION IF THERE IS A DISRUPTION OF POWER ON ESF BUSSES.

- OFFSITE CIRCUITS AND STARTUP TRANSFORMERS
- AUTOMATIC LOAD TRANSFER
- LOAD SHEDDING
- ESF LOSS OF NORMAL POWER LOGIC
- DG AIR STARTERS
- DIESEL GENERATORS
- DG LOAD SEQUENCER
- BATTERY CHARGERS
- STATION BATTERIES
- INVERTERS/MG SETS
- FUSING AND PROTECTIVE RELAYING

WHILE PLANT ELECTRIC SYSTEM CONFIGURATIONS DIFFER, THE SUCCESS OF THIS CHAIN OF SYSTEMS ASSURES POWER FOR ESFs.

HOW STUDY WAS CARRIED OUT:

- 1177 LERs (JAN 76 - DEC 78) PROVIDED BY ORNL
- LERs CATEGORIZED AS TO "KEY SYSTEM" WHICH FAILED
- CHECKLIST SHEETS PREPARED SHOWING HOW LER ITEM WAS IDENTIFIED
- CERTAIN LERs ELIMINATED AS TRIVIAL
- SIMPLE TRENDS NOTED
- COMPARISONS MADE TO WASH-1400 DATA BASE
- SIGNIFICANT EVENTS WERE SEPARATED OUT FOR DETAILED REVIEW
- POTENTIAL FIXES CONSIDERED IF NECESSARY

POOR ORIGINAL

MAJOR FINDINGS:

- DIESEL GENERATOR FAILURES ARE DOMINANT OES FAILURE (NO SURPRISE)
- FAILURES OF DG AIR STARTERS ROUGHLY 20% OF TOTAL

- A LARGE NUMBER OF OBSERVED SYSTEMS INTERACTIONS AND SEVERE TRANSIENTS ARE CAUSED BY INVERTER FAILURES
- KEY FACTOR WHICH MADE EVENTS MOST SEVERE WAS THE CHOICE OF AC LOADS ON SPECIFIC INVERTERS (E.G. COMBINATIONS OF CONTROL SYSTEMS)
- SIGNIFICANT IMPROVEMENTS IN INVERTER RELIABILITY NOT ANTICIPATED

- DC BUSSES PRESENT A MAJOR POTENTIAL FOR SYSTEMS INTERACTIONS
- VERY FEW ACTUAL EVENTS FOUND
- MOST ARE MAINTENANCE RELATED

- WASH-1400 RELIABILITY DATA APPEARS VALID (E.G. NO GLARING INCONSISTENCIES)
- OPERATOR ERRORS IN BREAKER OPERATION WORSE THAN WASH-1400

Table 4.0

Summary of Onsite Electric System Failure Modes, Consequences, and Potential Improvements based on LER Review

Failure Mode	Estimate of Occurrence Frequency	Consequences	Simplicity of Corrective Actions
Loss of Ofsite Circuits	-1/yr for single circuit -less than .25/yr all offsite circuits	-plant trip -shutdown via Diesel Generators	-Improvement in Power System Operating Procedures can yield only improvement -Additional circuits not cost effective -Natural phenomenon dominate as greatest source
System Undervoltage	-Rare (less than 1/yr)	-Disconnection and Load Shed, lead to plant trip -shutdown via Diesel Generators	-Adoption and adherence to strict guidelines for reactive load sharing would appear to be optimal solution
System Underfrequency	-Rare (less than 1/yr)	-plant trip via generator trip, loss of RC pumps, low RCS flow -shutdown via Diesel Generators	-Automatic Offsite load shedding on underfrequency to prevent excessive frequency decay is standard in US industry
Auxilliary & Startup Transformer Faults	-Very Rare	-ground & phase/phase faults accomodated by protective relaying -primary/secondary faults cause severe interactions on lower voltage side	-Systematic review of susceptibility of failure on low voltage systems would seem appropriate

POOR ORIGINAL

POOR ORIGINAL

Failure Mode	Estimate of Occurrence Frequency	Consequences	Simplicity of Corrective Actions
Switchyard Breakers and Autotransfer Logic Malfunctions (following plant trip)	-10^{-3} to 10^{-4} failure rate on demand, challenge rate from reactor trip ranges from 1 to 5 per year.	-potential loss of offsite power	-Achieving significant mechanical/electrical reliability improvements in breakers and logic is not realistic -potential areas for work: operating procedures, status monitoring to assure proper arming for transfer
Load Shedding Logic: -failure to shed loads -premature/spurious load shedding	-Rare -Rare	-aggravated undervoltage or underfrequency disabling of multiple ESF systems on train -loss of an ESF train leading to plant trip	-Logic in this area is already quite reliable
Diesel Generator Air Starters	-1/yr during tests or transients	-loss of one Diesel	-Addition of air driers to remove condensation -Increased surveillance to detect moisture and foreign matter in air lines -Improved air leak detection capability (Correction of Starter Malfunctions would eliminate 1/5 of all Diesel failures.)
Diesel Generators	-1/yr or more during tests or transients	-loss of one Diesel	-Provision of dust free enclosures and bifurcated contacts could potentially eliminate 1/8 of all Diesel failures. -Improved Maint., Test, and Operating Procedures could reduce next major source

POOR ORIGINAL

Failure Mode	Estimate of Occurrence Frequency	Consequences	Simplicity of Corrective Actions
Load Sequencer Malfunctions:			
-Incorrect Sequencer Timing	-Rare	-potential D.G. trip on overload	-Hardware modifications not viewed as cost-effective
-Timer Latchup	-Rare	-failure to power ESF systems in effected train	-Procedures to cope with failures viewed as most cost-effective
Battery Charger Trip	-1/yr or less	-No consequences if Station Battery is sufficiently charged	-Potential area for improvement is the use of lower charging currents in load discharge tests.
Station Battery Low Voltage	-less than 1/yr for most plants, frequent on others	-No consequences if detected and corrective action taken	-Improved procedures for transferring vital loads to backup transformer would be useful
Loss of a DC Distribution Panel	-Rare	-Severe Consequences: plant trip; loss of a single ESF train; inability to control AC breakers needed to restore power	-A majority of DC failures are human error related, thus operational QA procedures would be most useful -A system interaction study could identify the likely consequences and provide guidance
Inverter Malfunctions	-1/yr	-In B&W and Westinghouse plants vital bus inverter failures have been most severe. -Loss of Feedwater or Pressurizer Level Control has occurred on several occaisions	-System interaction review could pinpoint conequences and highlight optimal areas to modify.
Fusing and Protective Relaying:			
-Insufficient fusing	-less than 1/yr	-loss of large AC devices during testing	-Provide small instrument fuses on test jacks
-Incorrect Fuses/Relay Setpoints	-Rare	-loss of vital ESFs	-Improved operational QA

ITEM 1

AS RESERVE GENERATION DIMINISHES SHOULD MORE FREQUENT PLANT-GRID INTERACTIONS BE ANTICIPATED?

- IN THEORY: YES
- HOWEVER, RESERVE MARGINS ON A NATIONAL AVERAGE ARE ADEQUATE (SOME LOCAL PROBLEMS EXIST)
- THE CAPABILITY OF PERFORMING VITAL SAFETY FUNCTIONS CAN BEST BE ADDRESSED BY CONCENTRATING ON THE RELIABILITY ON THE ONSITE ELECTRIC SYSTEM RATHER THAN OUTSIDE GRID
- THE RELIABILITY OF THE OFFSITE GRID SHOULD BE VIEWED AS AN ENHANCEMENT TO THE RELIABILITY OF THE OES, RATHER THAN VICE-VERSA

ITEM 2

DURING CERTAIN TRANSIENTS CAN PROTECTIVE FEATURES INTERVENE IN AN UNANTICIPATED MANNER TO MAKE A TRANSIENT WORSE?

- IN THEORY AND BASED ON ACTUAL EXPERIENCE: YES

- MOST FREQUENT CASE: INCORRECT SETPOINTS

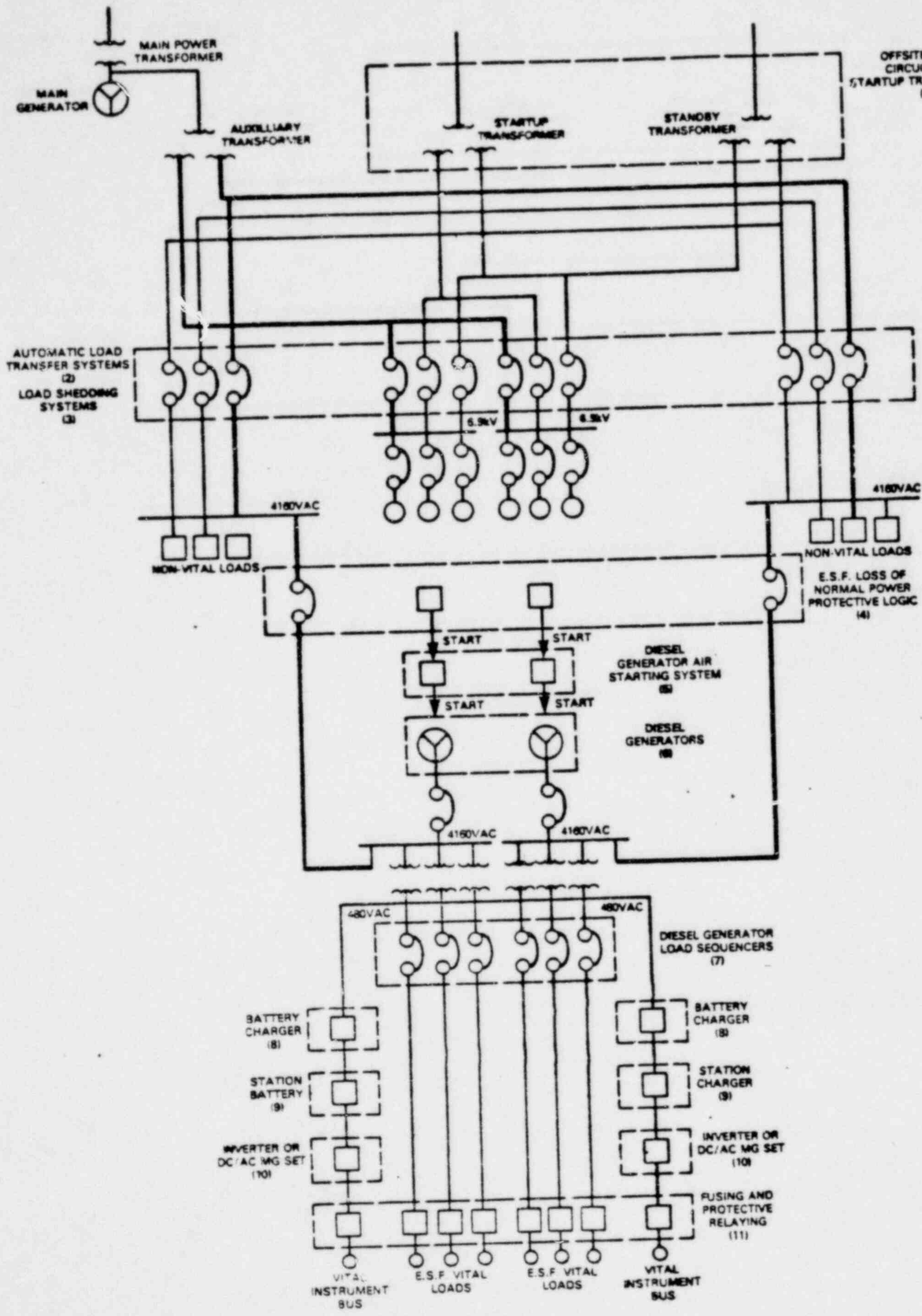
- TYPICAL: INCORRECT LOAD SHEDDING
  EXCESSIVE LOAD SEQUENCING CAUSING DG TRIP

ITEM 3

HAVE CERTAIN "COMPLEX" PROTECTIVE FEATURES YIELDED UNUSUAL PLANT OPERATING MODES WHILE UNDERGOING TEST AND MAINTENANCE?

- IN THEORY AND BASED ON ACTUAL EXPERIENCE: YES
- MOST FREQUENT CASE: PROTECTIVE INTERLOCKS ON SWITCHYARD BREAKERS

FIGURE I



POOR ORIGINAL