UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

- - -

PUBLIC MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON ELECTRIC POWER SYSTEMS

- - -

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

Friday, January 23, 1981

The subcommittee met, pursuant to notice, at 8:40 a.m.

BEFORE:

W. KERR, Presiding

J. C. EBERSOLE

WILLIAM M. MATHIS

JEREMIAH J. RAY

E. EPLER, ACRS Consultant

W. LIPINSKI, ACRS Consultant

ALSO PRESENT:

RICHARD P. SAVIO, ACRS Staff

- - -

P R O C E E D I N G S

MR. KERR: The meeting will come to order.

This is a meeting of the Advisory Committee on Reactor Safeguards, specifically, the Subcommittee on Electrical Power Systems - and a few other things, it seems to me.

My name is William Kerr, I am subcommittee chairman. Other ACRS members present, or who will be present today, are Mr. Ebersole, Mr. Mathis, and Mr. Ray. Our consultants present are Mr. Epler - who will be along presently - and Mr. Lipinski.

The meeting is the first in what we expect to be a series of meetings which is going to review the interaction of control and safety systems.

This meeting is being conducted in accordance with Provisions of the Federal Advisory Committee Act and the Sunshine Act. Richard Savio is the designated Federal employee. The rules for participation in the meeting have been announced as part of notice of the meeting published in the Federal Register on January 6, 1981.

A transcript of the meeting is being kept and will be available within five working days. We request that each speaker identify himself and use a microphone. We have received no written comments or requests for time to make oral statements from members of the public. We will proceed with the meeting.

I should call your attention to some correspondence that forms background for this meeting, copies of which you may have, the most recent being a letter from Mr. Ahearne, Chairman of the Nuclear Regulatory Commission, addressed to Mr. Placet(?) and dated December 12, 1980, with which Mr. Ahearne encloses copies of two letters from Congressman Udall.

One of these letters with which we will be concerned primarily in today's meeting refers to a previous exchange of correspondence between Congressman Udall and the Commission in comments as follows, this is in regard to instrument and control system failures that could initiate or exacerbate reactor accidents. "Your letter of November 17 and attachment thereto go a long way towards answering the questions I originally raised concerning this matter on February 7. I believe, however, that it is important that the Commission take further steps to provide assurance that judgments made over the years concerning the seriousness of this issue have not been re-affirmed without a careful re-examination of the foundations of such judgments.

"I am requesting, therefore, that the Commission ask the ACRS to review the staff's rationale on which its recent judgments relating to control system failures are founded, and that the ACRS report its findings to the Commission at an early date.

"As a specific part of the review I would hope that consideration be given to the specific concerns in this matter that have been expressed by staff which may not concur with the 'senior staff' referred to you in your letter of November 17.

"I would appreciate also that a report on progress in this area be presented when the Commission testifies early next year at the Interior Committee hearings on proposed legislation to authorize appropriations for the NRC for fiscal years 1982 and 1983."

There is another letter that deals with the ATLAS(?) issue, but this particular subcommittee, at least initially, will not look at that in detail, so I will not read that letter.

Mr. Ahearne's letter asks that the ACRS review these two questions, and that the committee provide a status report for Commission use in the congressional authorization hearings.

What I propose to do in this subcommittee meeting today is to get some initial comment from the NRC staff and to get comments from members of the subcommittee and the consultants as to an appropriate approach to this task.

One of the tasks that the committee has, of course, is to provide this early response to the Commission. To that end, I have prepared a draft letter which I would propose, after review by the subcommittee, to present to the committee, and to perhaps make it a part of the committee letter to Mr. Ahearne. I would want the subcommittee and the consultants to look at that draft later on and provide appropriate input.

But the purpose of today's meeting, from my point of view, is to solicit comments and suggestions from each of you so as to try to outline an approach to answering this request that we have from the chairman of the Commission and from Mr. Udall.

At this point I would solicit any additional comments from members of the subcommittee, if you want to make any at this point, or questions. Mr. Ebersole?

MR. EBERSOLE: We were just talking a while ago. I think there are two courses of action here. One that has been recommended is that we study the dynamics of control systems in great detail and, I understand, very thoroughly indeed, the potential for control system reviewing or imposing on whatever parameters they control unsafe rates and aptitudes of control, a massive task to undertake.

I think what happened in the industry really has been that the parameters to be controlled by control systems have been in many cases not recognized as having a safety context. I will just pick one of these, for example, that is the secondary site level which, I think, we all know and have lots of papers to study about. We now know it to be a substantial safety issue.

It has been many years since we have tried to get the industry to put hard controls, overriding safety controls, on such things as boiler overfill, excessive main feedline flow, main feedwater flow. We know of the B&W analysis that there is a substantial accident potential here, I understand from the thermo-shock aspects of this, coupled with potential for loss of main steam lines. That is probably the issue that is keeping Great Britain from building American reactors, the thermoshock potential on the vessel; the combined potential for losing the secondary circuits by virtue of overloading the main steamline on B&W plants.

I think an alternative approach to what Mr. Basdekas, I think wants, which is intensive study which I certainly recommend if we can do it, of the control systems essentially to carefully identify the potential range and rates of the parameters of interest in uncontrolled systems and, where necessary, superimpose safety systems to cope with those ranges in rates as appropriate. I think that is an alternative approach.

We now know from experience that it was control systems, in fact, that were causing us trouble, the duct and vent valves and in this case a misapplication or maldesign of float switches. That is another case of a somewhat different character.

But I think that is a possible alternative, is to look at the limits of rate and aptitude of all system parameters to safety and, where appropriate, where we have not yet done so, apply safety controls fully "church in character" as Mr. Epler would say, capable of coping with those rates and aptitudes that might be imposed on those parameters by the safety control system.

That is all I have to say.

MR. KERR: Thank you, Mr. Ebersole. Mr. Mathis?

MR. MATHIS: I don't have any particular comments at this time, Bill.

MR. KERR: Mr. Ray?

MR. RAY: No comments, but I have a question. Will we hear in this presentation as scheduled by the staff what steps have been taken by them in the interim, in view of these incidents that have occurred in operating plants?

MR. KERR: I don't know the answer to that. I did not give the staff very specific instructions about the presentation. So, I don't know. But this, I would assume, is the first of several meetings and what I hope that we will do as a result of today's meeting is to be able to give the staff a better idea of what we would like to hear from them.

So, if you don't hear something that you would like to hear, I think today's meeting will form at least a place from which requests can come.

Mr. Epler, do you have any comments?

MR. EPLER: I think we could have answered this letter 35 years ago very simply by saying, we recognized at that time that you cannot fix all the things that can happen to control systems. It is an endless job. You have to review everything in the plant down to the nearest one-tenth of an inch to identify the safety problems. Having identified the problems, we are putting in protection systems to make sure we cope with them. We will separate the safety system from all nonsafety systems as best as we can - not perfectly, of course - and make sure that we optimize each for its intended purpose - optimize the control system to control, if that is its function; optimize the protection system to protect. That is the best we can do.

Now, we can spend the rest of our lives nitpicking pieces of this, but it won't get us very far.

MR. KERR: I hope we have a record of that because we could use that as one draft of a letter.

(Laughter.)

MR. KERR: Mr. Lipinski?

MR. LIPINSKI: I have to disagree with Mr. Epler. Part of it is right.

MR. KERR: That would be the first time anyone ever disagreed with Mr. Epler.

(Laughter.)

MR. LIPINSKI: Our experience, starting with TMI and several incidents following that, there are certain design principles that have been disregarded in the design of control systems, and in control I will clasify the automatic systems as well as the manual systems.

I would agree that we have to look at the rates at which the variables change, what their magnitudes are. But if you do this one variable at a time you may get a conservative analysis.

MR. EPLER: I didn't say that.

MR. LIPINSKI: OK. I am going to add, you then have to look at the modes in which the control systems can fail. I would not just look at the outputs from the controllers but where they share common power supplies, mainly where an integrated controller loses his input information because his sensors went out. It opens up the power operated relief valves; the control cuts out and cuts off feedwater. Everything went in the wrong direction, three variables simultaneously, and then blacks out the panel for the operator so he can't tell where the plant is at.

So that somewhere we need some design guides in terms of how many failures are acceptable in terms of the control system failure.

MR. KERR: Mr. Ebersole?

MR. EBERSOLE: I want to extend your observation and say something else. There is an analogy between our control problem here and many service systems, one of which we were talking about yesterday.

I would like to extend the scope of the control system right out into the service system and say that it is my view that the service systems, I will call them in the nonsafety context of the plant, like DC power, or like service water, or AC power, should be kept isolated and taken in the control context or service context.

We then park to one side of the redundant safety grade systems which will mitigate malfunctions of those systems. A case in point is the two-chennel DC system. When you lose one side of that, you lose the control functions that go with it. You lose the mitigating functions that go with it. You have no redundancy to meet the current events.

It has not been a generic, thorough policy of NRC to identify in totality the service function of a plant, park it to one side and then clearly separate the overriding safety functions on another side of a wall. Ultimately, I think, we must come to that.

That takes one working train. It takes two trains to back up its malfunctions wherever you go, without having them meet somewhere in the middle.

MR. LIPINSKI: I would like to add to my earlier comments. Based on these experiences, the NRC has certain remedies in process right now to solve some of the problems that have occurred. I do not want to imply that nothing is being done. We have learned from these experiences.

MR. EPLER: It is being whittled at.

MR. LIPINSKI: It is being whittled at. But the question is, do we have a systematic approach to the total problem.

MR. EPLER: Just for the record, I want to point out that Walt Lipinski and I don't disagree a bit. He said in a great many words what I said when I said, identify the problem. You have to identify the problem in order to build an effective system. Sure, you have to look at what you can do, but you don't try to fix them.

MR. KERR: I think the comments that we have heard are perhaps illustrative of ours and Mr. Udall's problem. I am not sure whether we want to answer Mr. Udall's letter or, maybe, answer another letter that he should have written and did not. We will have to give it some thought. But this is probably enough and I think these comments are relevant to the problem.

What we eventually have to do as a committee is to try to pick out from the accumulated wisdom that part that should be used in responding to the letter, I guess.

We have with us this morning representatives from the NRC. In our discussions with them we did not ask that they make a detailed, formal presentation, but rather that they make whatever presentation they felt would be helpful to us generally, if they want to make one and be available to make contributions to the general discussion.

I am told that Mr. Faust Rosa who was recently appointed branch chief - an exalted position - for instrumentation and control has with him his capable assistants. I am going to ask Mr. Rosa to begin the discussion and give us some input from the NRC staff.

Incidentally, if you want to sit around the table or there, whatever, this is going to be a fairly informal meeting, and whatever geographical and oral presentation you want to make will be appropriate, Mr. Rosa.

MR. ROSA: Thank you, Dr. Kerr, and ladies and gentlemen. This is Faust Rosa.

Within NRR, I guess, it is accurate to say that the responsibility for this issue has been assigned to the Instrumentation and Control Systems Branch. Within that branch, it was assigned to Dr. Ernie Rossi, a senior member; and he is going to make the presentation. He is going to be supported as deemed necessary by Dr. Morris here, Bill Morris and other members of the staff who have elected to come down here and be in attendance.

Therefore, without further ado, Ernie Rossi will start his presentation.

MR. ROSSI: I do not have any slides this morning. What I would like to do is to summarize the status of the NRC control system reviews, the way we have done those reviews in the past.

I would like to try to tell you where we have drawn the line in limiting our reviews. The discussion of conrol system failures can be divided into the following considerations.

MR. KERR: Excuse me, Dr. Rossi. You have copies of the correspondence that has led to this discussion, I take it?

MR. ROSSI: Yes, I do.

MR. KERR: Are your remarks, if I can try to separate them, aimed at what you deem to be an appropriate answer to these letters, or are you sort of talking to the general topic of how you have up to now treated the review of control systems?

MR. ROSSI: I think my comments are directed towards a summary of how we have treated control systems. At the end I am going to summarize the actions that are currently under way that address the problem.

So, really, what I am trying to do is to help everyone better to find the problem and also to tell you what actions are under way at the current time, and what actions are planned to address the problem.

MR. KERR: Thank you.

MR. RAY: Question?

MR. KERR: Yes.

MR. RAY: Those actions that are under way are attuned to the incidents that have developed in the plants in recent months?

MR. ROSSI: They certainly arise out of those in some cases. In some cases they arise it is just a re-emphasis of things that were, in my opinion, already under way within the NRC.

The discussion of control system failures I have divided into three considerations:

The effects of control system failures on anticipated operational occurrences.

The effects of control system failures on accidents.

The effects of control system failure on operator actions.

The operator actions would be considered with the plant at shutdown, during plant heatup or cooldown, following plant trips, or following the actuation of engineered safeguard systems. The control system failures might include those which deprive the operator of required information for manually controlling plant conditions, failures which provide confusing or incorrect information to the operator, or failures which may initiate or compound the transients.

First, let's consider the effects of control system failures on anticipated operational occurrences.

The NRC staff reviews have been performed on currently licensed plants with the goal of ensuring that control system failures will not prevent automatic or manual initiation and operation of any safety system equipment required to trip the plant or to maintain the plant in a safe shutdown condition following any anticipated operational occurrence or accident.

The approach has been to either provide independence between safety and non-safety systems or to require isolating devices such as isolation amplifiers between safety and non-safety systems such that failures of non-safety system equipment cannot propagate through the isolating devices to impair the operation of the safety system equipment.

In addition, a specific set of "anticipated operational occurrences" have been analysed to demonstrate that plant trip and/or safety system equipment actuation occurs on a time scale such that no core damage results.

In these analyses, conservative initial plant conditions, core physics parameters, and instrumentation setpoints have been assumed. Conservative core parameters, that is heat fluxes, temperatures, pressures and reactor flows which could result in core damage have also been assumed.

Where active control system operation would mitigate the consequences of the transient, in general no credit is taken for the control system operation. No penalties are taken in the analyses for incorrect control system actions caused by control system equipment failure.

The operator is assumed to not intervene with actions which would mitigate the consequences of the transient for at least the first few minutes - typically at least ten minutes. No penalties are taken in the analyses for incorrect manual operator actions.

Now, in the case of control systems this means that the loss of forced reactor flow, for example, is analyzed assuming that the reactivity control systems either operate properly or do not operate at all, whichever is the worst case.

A loss of forced reactor flow occurring simultaneously with an inadvertent rod withdrawal is not considered. Now, among the specific set of "anticipated operational occurrences" that are analyzed are occurrences resulting from both mechanistic and non-mechanistic control system failures. We would like to leave the emphasis being on the nonmechanistic failures.

The conservative analyses performed and the "anticipated operational occurrences" chosen for analyses are intended to demonstrate that no core damage occurs for a wide range of bounding events which might occur on a frequency of once or more during the life of a plant, even though specific events might not follow the same conservative assumptions that have been made in the analyses.

Now I will summarize the possible problem areas in the approach. This also summarizes, I think, where we delimited the approach that we take with control systems.

No systematic evaluation of control system designs has been performed to determine whether single failure induced multiple control system actions could result in a transient such that core limits established for the anticipated operational occurrences are exceeded.

MR. KERR: Excuse me, what was that, something initiated multiple something or other?

MR. ROSSI: Yes. That is, no multiple control system failures that might be initiated from a single cause, such as a power supply. Now, we have not systematically gone and looked for every one.

MR. KERR: I just wanted to understand what you say. I am just trying to get the statement. I was not even able to piece together the statement. Would you read it again, please?

MR. ROSSI: Sure. No systematic evaluation of control system designs has been performed to determine whether single failure induced multiple control system actions could result in a transient --

MR. KERR: Single failure induced multiple --

MR. ROSSI: Actions.

MR. KERR: Tell me what a single failure induced multiple action is.

MR. ROSSI: OK, let me give you an example. As a matter of fact, I believe this is an example that would not exist anywhere, but I just indicated to you that we did not analyze the loss of reactor coolant system flow simultaneously, assuming a rod withdrawal accident.

Now, if there were a single failure some place that could cause those two things to occur at the same time, that would be a mechanistic single failure that would lead, perhaps, to multiple control actions, the multiple actions being withdrawing the control rods inadvertently at the same time that you for some reason reduce the reactor coolant system flow inadvertently.

I am saying that we have not systematically gone through the control systems to look for all of those cases.

MR. KERR: Where a single failure in the control system --

MR. ROSSI: Causes multiple actions.

MR. KERR: Now, do you look for some single failures that cause single actions?

MR. ROSSI: Well, that gets to the question of whether our analyses are mechanistic or not mechanistic. We have things like a rod withdrawal accident that is analyzed, and we have another accident, a separate one, that is analyzed, which is the loss of reactor coolant system flow.

Now, In general we do not try to identify all of the things that could cause those. So, you analyze those as severe control system malfunctions where we don't go back and try to identify all the specific things that might cause it, but then we use very conservative analyses in analyzing each of those individually.

MR. KERR: So a short answer to my question, it might be sometimes.

MR. ROSSI: I think that is fair.

MR. LIPINSKI: Mr. Chairman?

MR. KERR: Yes, sir.

MR. LIPINSKI: The speaker may correct me, but I believe we have this presentation as an attachment to a memorandum dated December 4, 1980 from Denwood Ross.

MR. KERR: Are you reading from that?

MR. ROSSI: To a large extent I am. I do not intend to go through all of that.

MR. KERR: Well, there may be members of the subcommittee or consultants who can't read.

(Laughter.)

MR. ROSSI: I have also made some changes to that. What I intend to do is not to go exactly through it. I think you have found that already, perhaps.

MR. RAY: Question. In these instances where you have a single reaction, do you then make a systematic study?

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

MR. RAY: Well, you said no system study is made, or no systematic study is made in the incidents that cause multiple control responses. Do I read you right on that?

MR. ROSSI: We have not done a systematic study to identify all the multiple responses that might be caused by one single event or failure; that's correct.

MR. RAY: Well, in the event of a single control response to an incident, do you make a study of a whole control system? Is that a systematic study, or is it a study of the isolated hardware?

MR. ROSSI: Let me go back to the rod withdrawal accident again. We analyzed inadvertent reactivity insertion from control rod withdrawal. Now, in analyzing that, the assumptions that go into that accident analysis would look at the control system sufficiently to ensure that the reactivity insertion rate which is used in that analysis balanced anything that the control system could realistically do in single failures.

MR. RAY: So that any perturbations beyond would be recognized as a result of that type of study.

MR. ROSSI: But only in that reactivity insertion, we would not go back and systematically look to see if, for example, a relief valve might open at the same time; that we would not do.

MR. RAY: But if the perturbation that you are concerned with could influence something else in a logical sense.

MR. ROSSI: Oh, yes, right. In general, if other control systems by doing the thing that they are supposed to do, would do something bad, that would be taken into account. If the other control systems by doing the thing that they are supposed to do would mitigate the consequences of the transient, then in general the assumption would be that those control systems are essentially manual so that they don't act to mitigate.

But what we don't do is go and look for other failures of other control systems that might cause wrong control actions because of additional equipment failures.

MR. RAY: But actuation that leads to an independent event, not related to the one you are concerned with.

MR. ROSSI: Yes, although we still have probably not systematically tried to look for single failures that might cause a multitude of control actions.

We have a lot of reasons to believe that they don't exist in very many places, but we have found some from time to time.

MR. MATHIS: May I ask a question? How can you say that when you use common power supplies, such as DC power supplies, or a multiplicity of control stations the common failure of which involves the failure of that control system, which was one branch of its mitigating function and possibly other control systems?

MR. ROSSI: That only becomes a problem if the power supply failure causes an inadvertent control system action. Now, if a power supply failure were to cause the rods to be inadvertently withdrawn or cause valves to initiate transients, then that would be a problem.

MR. EBERSOLE: Do you analyze those common power supply failures to control and safety systems which come from the same source?

MR. ROSSI: I would say that we have analyzed the commonality to make sure that something like that would not cause a transient, and at the same time to feed the protection for that transient.

MR. EBERSOLE: Like Crystal River?

MR. ROSSI: Crystal River, that was a multitude of control system failures. I do not know that it defeated any trip actions at the same time. But I am not that familiar with it.

MR. EBERSOLE: When you said "trip actions" you lost me because tripping a reactor is vastly simpler compared to the follow-on actions that must be done after the tripping function.

To this extent I think that the follow-on action which is persistence of the removal function and in particular those aspects of secondary circuit design have been given pret. much short shrift in the control and safety analysis area.

MR. ROSSI: Well, I would have to say that certainly systematic reviews of the control systems and what even power supply losses might do to the control system, in a systematic way I would say that that has not been systematically done.

MR. EBERSOLE: Thank you.

MR. ROSSI: But we have addressed problems that we find in our reviews or problems that occur from incidents, we try to look beyond those and address the issues. But we have not done the systematic kind of review that we would do, for example, for a safety system.

MR. EPLER: Question. I am not sure of the ground rules here. When you say a "control system" do you mean specifically the systems for dynamic control, or do you mean all non-safety systems?

MR. ROSSI: I am using "control systems" here to really mean the instrumentation and control systems that are non-safety systems.

MR. EPLER: Just the instrumentation.

MR. ROSSI: Just the instrumentation.

MR. EPLER: Well, this is rather narrow in scope.

MR. ROSSI: It is somewhat, yes. It does not include a lot of mechanical equipment.

MR. EPLER: It does not include the roof falling in, for example.

MR. ROSSI: Beg your pardon?

MR. EPLER: It does not include the roof falling in.

MR. ROSSI: That's correct, that is a good example. If you have a nonseismically qualified building I would not include the building.

MR. EPLER: It would give you a lot of failures. So, we are restricted to those instrument failures that could cause a dynamic control system to produce undesirable action.

MR. ROSSI: Right.

MR. KERR: Please proceed, Mr. Rossi.

MR. ROSSI: OK. It should be emphasized that the primary issue is not whether reactor trip or safety system equipment action would be defeated, but whether trip or equipment action would occur in time to maintain the core design limits appropriate for "anticipated operational occurrences" and, perhaps more importantly, whether control system failures might confuse the operator such that he takes improper actions which worsen the transient consequences.

We believe that systematic reviews of safety systems have been performed with the goal of ensuring that control system failures - either single or multiple - will not defeat trip or safety system action.

Now, what we mean there is that where we use isolation amplifiers that we put a lot of effort into making sure that regardless of how many things go wrong after the isolation amplifier, and how it goes wrong, that that will not keep the safety system from either tripping the plant or actuating safety system equipment that might be needed during an "anticipated operational occurrence" or accident.

MR. RAY: In the analysis that you just mentioned, do you consider the level of the load on a reactor as having any influence on that interaction?

MR. ROSSI: The level of the load?

MR. RAY: For instance, a hundred percent of load on the reactor.

MR. KERR: The power level of the reactor, I think.

MR. ROSSI: Yes, we look at a multitude of power levels. For example, going back again to the rod withdrawal accident, the rod withdrawal accident is looked at, at power levels all the way from way down in source range, the lowest that you could ever get to in terms of the initial neutron level, all the way up to the maximum power level that the plant could ever operate at.

In addition, we look at the reactivity insertion rates. We don't just look at the maximum possible rate. We look at a whole range of rates from, you know, minimal insertion rate all the way up to the maximum possible that could occur. So, we try to bracket that analysis in both power levels that we look at, by looking at a wide range; and also in the reactivity insertion rates.

MR. RAY: To make sure I understand your response, you consider this range of power levels in a reactor in your investigation of the integrity of the isolation between the control system and the protection system.

MR. ROSSI: Right.

MR. RAY: And make sure that that integrity is not different, if you will, or deteriorated as a function of the power level in the reactor.

MR. ROSSI: That is correct, yes.

MR. KERR: Would you go back and read for me what you said the issue was because before you emphasized that the issue is something or other.

MR. ROSSI: I think I didn't really say what the issue was - maybe I did. I said that it should be emphasized the primary issue is not whether reactor trip or safety system equipment action would be defeated, but whether trip or equipment action would occur in trying to maintain core design limits appropriate for anticipated operational occurrences and, perhaps more importantly, whether control system failures might confuse the operator such that he takes improper actions which worsen the transient consequences.

MR. KERR: Now, to what issue are you referring when you say this is a primary issue?

MR. ROSSI: Well, I am saying that we feel that we have done a lot of review to make sure that control system failures won't keep the plant from tripping or keep you from actuating safety system equipment.

We have not done systematic reviews to make sure that control system failures can't cause a multitude of control system actions which might cause transients to go in a less conservative way than analyzed, such that you violate, perhaps, the limits that you have set for anticipated operational occurrences.

So, you would always trip and you would always actuate safety system equipment, in my judgment. What you might have a problem with is that the times might be a little different than what has been analyzed in the safety analyses reports.

MR. KERR: I could reword that, then, to read that the basis for the staff's approach to the review is, the foundation for your review is based on --

MR. ROSSI: The separation of safety systems and protection systems from control systems.

MR. KERR: OK, I think I understand.

MR. EBERSOLE: By and large your emphasis has been on core protection, of course, for many years; that has been one of the principal emphases.

Are you now having a look, as a mechanical engineer must be, at the implications of secondary system couplings, the potential for permanent mechanical damage of gross character, leading in the long term to core damage of a very severe type?

I can use as a model for this the secondary transients that I referred to earlier.

MR. ROSSI: You are concerned about thermotransients on a vessel, that type of thing?

MR. EBERSOLE: Right, reflecting eventually on the core, but not immediately.

MR. ROSSI: I am not terribly familiar with those, but they are done. Accident analyses are done where you identify cooldown rates which occur in the reactor coolant system, and then those are taken back and looked at in terms of the stresses on key components.

MR. EBERSOLE: Well, it is a case in point at this point in time. I think there is only beginning consideration of the potential for loss of level control in secondary circuits.

MR. ROSSI: For filling, for overfilling.

MR. EBERSOLE: Yes, correct.

MR. ROSSI: I think that is probably true on your over-filling or not having enough flow. I think that has been systematically addressed in fairly much detail. I think that you are right, that there are areas that could be addressed in more detail on excessive flows of feedwater.

MR. EBERSOLE: When I said, by the way, a while ago "range" I meant into the range.

MR. ROSSI: I understand. I am sure there is no question in the accident analyses that some ranges have been looked at in more detail, for some accidents, than perhaps others.

On the feedwater flow, I think the stress has been in the past on making sure that you have enough feedwater flow, and there may have been some areas that deserve more attention on problems you might get into with too much.

MR. EBERSOLE: Right.

MR. LIPINSKI: I would like to back up to your statement on separation of protection and control. It is a desired feature, but if I recall you do not require it because there are designs now for protection channels on instrumentation assured with the control channels.

MR. ROSSI: Yes, but that is done through what are called isolation amplifiers where any failure on the non-safety system side cannot propagate back through the isolation amplifier into the safety system to defeat the safety system.

MR. LIPINSKI: That takes care of the electrical signals but in terms of the shared information a channel failure, not giving you availability of that protection channel, could lead to a control system failure in the direction that gives you a challenge.

MR. ROSSI: That issue has also received considerable emphasis in the past. That is a case where, for example, a detector that supplies the signal for both the control system and the protection system fails. By that detector failing it causes a control system malfunction that leads to an accident. It also defeats one protection system channel.

The criteria is - and it is a well-understood criteria - that the remaining protection system channels, assuming that the detector that is common has defeated one protection system channel, that the remaining channels still have to meet the single failure criterion. That is certainly a criterion in IEEE 279.

Considerable effort has gone into that issue over the years.

MR. EBERSOLE: In deriving your signal from the parameter of interest at its source, does your area of interest extent right on down into where you tap the primary process to include verification of the fact that you don't manifold center lines, or impulse lines, or hitters?

I have seen control systems in which virtually all parameters of interest have been tapped out of a common manifold. All you had to do was knock off the manifold and go completely blind.

MR. ROSSI: Well, they should have been done, and I think the criteria covers that. I would not be familiar enough with all the reviews to be able to say that they systematically have been looked at in every case. But in my opinion the criteria for that comes under the same thing we were talking about, that if you have a single failure that affects both the protection system and the control system, the protection system that remains after that failure is supposed to still be able to meet another random failure and protect you.

MR. EBERSOLE: But does your domain include actual tapping of the primary process by whatever mechanical means you use to do that?

MR. ROSSI: I believe it does, yes.

MR. EBERSOLE: I am afraid you might just stop at the --

MR. ROSSI: I don't think that is the case, but I could not personally verify it.

MR. ROSA: I think that we can state with assurance that it does. The criteria will take us all the way down to the sensor.

MR. EBERSOLE: You said the sensor. I want to go beyond.

MR. ROSA: Even beyond. You are talking about a common manifold.

MR. EBERSOLE: Or impulse line.

MR. ROSA: Or impulse line. I can say right now, yes, the criteria will take us all the way.

MR. EBERSOLE: There are lots of old plants in place.

MR. ROSA: There may be some old plants in place where there is common manifolding.

MR. EBERSOLE: We knock off a manifold, we are in big trouble. It is a small line, it is easy to break. It introduces compounded effects.

MR. ROSA: It is, of course, a problem. The extent of the problem I don't know. I believe when those old designs were reviewed and approved, this common manifolding was considered, was recognized and considered, and was approved on what was then an acceptable basis. Since then, the criteria have been revised to be more stringent.

MR. EBERSOLE: Let me tell you what that basis was, it was that a small leak is not important.

MR. ROSA: I believe that is right.

MR. EBERSOLE: That is not valid.

MR. ROSSI: I think in the original protection, or at least in the more recent protection systems - I can't say the original ones - but I think that has been addressed in the designs where they share tasks; that is what I believe.

But I would be unable to personally verify that there has been a systematic study to look for all of them. But I believe the criteria certainly addresses it and any time I looked at a problem like that, I would consider that, I personally.

MR. EBERSOLE: That's today.

MR. KERR: Is your question aimed at whether the criteria are appropriate, or whether they are being applied appropriately? I am not sure.

MR. EBERSOLE: The criteria we have today may well cover this, but we may have lots of plants in place --

MR. KERR: Your question is, have existing criteria been applied to all plants.

MR. EBERSOLE: Yes.

MR. ROSSI: And in a systematic way.

MR. EBERSOLE: Right.

MR. ROSSI: With a systematic review.

MR. KERR: You can answer that question with at least 99 percent certainty.

MR. EBERSOLE: No. Right?

MR. KERR: Yes.

MR. EBERSOLE: Well, I think that is a hanging hazard that should be investigated.

MR. LIPINSKI: Let me add to that, IEEE 297 covers all the electrical systems.

MR. EBERSOLE: Only.

MR. LIPINSKI: Only. At one time there was to be an equivalent standard from the mechanical people which was never produced.

MR. EBERSOLE: Right.

MR. LIPINSKI: To make sure that the totality of protection from all the mechanical components and electrical components existed.

MR. KERR: Those mechanical engineers had better get on the ball.

MR. EBERSOLE: Therefore, there is a window through which all sorts of safety problems can occur.

MR. LIPINSKI: That's correct.

MR. EPLER: Mr. Chairman, I think this discussion should take into account not only what has just been said, but take into account the fact that IEEE 279 tends to legalize designs wherein control and protection instrumentation is shared by invoking the single failure criteria. It does not recognize, as Jesse has said, manifolding or common mode failures. It assumes that the failures will always be single failures.

Now, this was opposed rather vigorously at the time the standard was written, but has not succeeded in getting it out because it was kept in to legalize some existing design.

I would have to say that we do recognize common mode fail:res. You will have blinding of all sensors and this causes the accident and protection failure to occur at the same time, which is entirely undesirable. But, we are living with it.

MR. KERR: Thank you, Mr. Epler. Mr. Rossi?

MR. ROSSI: If single failure or single event induced multiple control system action, such as I discussed previously, do indeed exist. We believe that the experience with operating plants indicates that these kinds of incidents that might result in transients that are more severe than currently analyzed as anticipated operational occurrences, have a low probability.

What I am saying is that we do not have evidence from the operating plant experience that would indicate that we are seeing real failures of plants that are causing anticipated operational occurrences that go beyond what we have analyzed as anticipated operational occurrences.

MR. KERR: Excuse me, let me make sure I understand your last statement. You are saying in effect that you don't think you missed many important things because if you had, they would have shown up in operating experience by now.

MR. ROSSI: That is basically what I am saying.

MR. KERR: OK.

MR. ROSSI: Many plants have trips that are based upon a combination of primary system parameters, such as power, temperature, pressure, such that any steady state combination which would result in exceeding core limits for anticipated operational occurrences would yield a trip.

Control system failures affecting any or all of those parameters used in this type of trip are thus, at least to some extent, addressed.

However, simultaneous control system failures that could conceivably result in a faster transient with a time response such that the core limits for anticipated operational occurrences might be exceeded.

However, it is likely that the core limits would be exceeded by only small amounts and for only a short period of time. This is likely the case even if a plant does not have a trip based upon a combination of parameters affecting core limits.

Now, we have a lot of plants that have trip set points where you trip at a power level in a core that is a function of the reactor coolant system pressure and the reactor coolant system temperature. Those trips would be set up so that when you got to any steady state condition on that trip line, that the core limits would still be maintained.

Then, to use those trip limits in the particular analyses that are done, and you show that for those particular analyses the time responses are adequate to make sure that you stay within the specified core limits.

Now, where the limit is drawn is that we don't look for a multitude of control system actions were it might cause the transient to proceed at a faster rate because you have many things now going wrong. Where the transient might proceed at a faster rate than what has been analyzed, we have not looked for those. Is that clear?

We have many plants and not all of them have these kinds of trips. Many plants have trips where the power level trip is a function of pressure and temperature. You set those trips up and you look at specific, for example, rod withdrawal accidents and you do this range of rod withdrawal accidents and a range of power levels to show the time responses are adequate to keep you within the specified core limits.

Now, where we draw the line is again, we don't go back and see a rod withdrawal accident, a loss of flow, a pressurized relief valve all opening at the same time and try to prove that for that worst case the transient proceeds at a rate where the core limits are still maintained.

MR. EBERSOLE: A while ago you mentioned over power transient, and you expressed the desire that the pumps not stop.

MR. ROSSI: Well, what I indicated was that the analysis was done with the assumption that they do not.

MR. EBERSOLE: Well, let me follow it up a little bit. When you have a reactor trip most designs require that you execute a turbo trip. That is a cessation of power flow to the main coolant pumps which must be restored or transported to some other source. A transfer that may be missed and in fact is sometimes denied as impossible - you know, the off-site power failure coincident with that turbine trip, an instantaneous cascade.

Do you permit a core design that can suffer damage when in fact you suffer an over-power transient due to rod withdrawal and you do trip the pumps at the same time?

MR. ROSSI: If we knew that the pumps were consequentially being tripped as a result of the reactor trip on a time scale where, you know, you could lose flow at the worst point in the transient, we would not permit that.

MR. EBERSOLE: Do you permit transfer to a presumably available other source and then allow the design to proceed?

MR. ROSSI: I am not sure I can answer that question as to whether that would have ever been permitted.

MR. EBERSOLE: I know of one design, I believe it is Westinghouse, that demands that you don't order transfer but follow up on the turbine to, presumably, prevent core damage, by running the risk of failing to order transfer.

MR. ROSSI: There is a delay in there on that transfer, I believe, on some plants in order, certainly, to strengthen the assumptions that have been made so that you don't have to go back and try to argue that when the flow loss is occurring with respect to the trip.

But I would like to point out that when you trip that the rods go in at a fairly rapid speed, and that turns that transient around very rapidly. So, you have to have the loss of flow during a very narrow time window there in order to exceed the limits for the anticipated operational occurrences, and then you come back.

I mean, it would have to be within that very narrow window.

MR. EBERSOLE: Well, that is where it would be, in fact.

MR. ROSSI: Not necessarily because it takes some time to trip the ractor, you trip the turbine. There are seconds involved in there, in general and you are talking about a pretty narrow time window.

MR. EBERSOLE: Well, you do permit designs that require continuity of power flow to the cooling pumps in order to mitigate, to prevent core damage; do you not? Relying not totally on flywheel action.

MR. ROSSI: I think that is correct, yes. I can't speak to that question with a lot of confidence that I know the answer to it.

MR. ROSA: If I might interject, I don't know for certain, but I believe that all accident analyses assume loss of off-site power simultaneously with the accident, that is true.

MR. ROSSI: That is for the accident, that is correct.

MR. ROSA: That means that the main coolant pumps, or course, are tripped at the same time. Now, as far as transients are concerned, I would expect that if you had an over-power transient which caused the trip, its analysis would also assume that the off-site power was lost.

MR. ROSSI: But it does not assume that the flow is lost at the time, the key point in the rod withdrawal.

MR. KERR: Let me suggest that this is a level of detail that is certainly important to accident analysis. We want specific information, so we should ask the staff for answers.

But I think it is perhaps a little more detail than we need for the specific question with which we are dealing. It is a very important question, certainly, for a specific accident analysis. Mr. Rossi?

MR. ROSSI: I would like to say one more thing on that question, and that is that the attempt is when we do accident analyses that you do include all of the consequential things that occur from the accident; that is the intent.

Your question, I think, may involve the degree to which it has been systematically verified that that has been done.

Now, let's consider the effects of control system failures on accidents.

MR. KERR: Mr. Rossi, it sounds to me like this is a transition point, and if it is, I am going to declare a ten-minute break. Is it?

MR. ROSSI: Yes, this is a good spot.

MR. KERR: All right, I will declare a ten-minute break.

(Whereupon, at 9:35 a.m. a short recess was taken.)

MR. KERR: May we reconvene, please. Mr. Rossi, you have a small but dedicated audience. Please, continue.

MR. ROSSI: You want me to start now?

MR. KERR: Yes.

MR. ROSSI: I talked about the way control systems are dealt with for the anticipated operational occurrences, and where we have drawn the line, and what we have looked at.

Now, why we consider the effects of control system failures on accidents or limiting faults.

It has been noted at this point several times, NRC staff reviews have been performed on currently licensed plants with the goal of ensuring that control system failures - either single or multiple failures - will not prevent automatic or manual initiation and operation of any safety system equipment required to trip the plant or maintain the plant in a safe shutdown condition following any anticipated operational occurrence or accident.

In addition, a specific set of "accidents" has been analyzed to demonstrate that plant trip and/or safety system equipment actuation occurs with sufficient capability and on a time scale such that the potential consequences to the health and safety of the public are within the acceptable limits for that accident.

As with the anticipated operational occurrences, conservative assumptions are used in those analyses. The conservative analyses performed and the accidents chosen for analyses are intended to demonstrate that the potential consequences to the health and safety of the public are within acceptable limits for a wide range of postulated events, even though specific actual events might not follow the same assumptions made in the analyses.

Again, this comes back to the fact that we pick particular accidents to look at which we feel are the most severe that would ever occur, and that is intended not to try to predict how an accident might really occur, but be a limit that we can analyze which will bound anything that might occur, even though the things that might really occur would follow a somewhat different sequence.

Now, I will summarize the possible problem areas.

MR. RAY: Question. These accidents that you refer to are postulated. Do you ever examine those in the light of an actual occurrence subsequent to your reviews to ensure that you have in truth found that you have experienced a situation that exceeds the limits that you had?

MR. ROSSI: Yes. Any time there is an event at a plant, those are reported to the NRC, and one of the things that is done in looking at the event is to look and see if the event means that the accident analysis is not valid. That is a continual thing that is done.

We have presumably a fairly significant amount of effort that looks at the licensee event reports and relates those to what we are really doing within the NRC in terms of the reviews and the analyses.

In the area of accidents, systematic evaluations of control system designs have not been performed to determine whether postulated accidents could cause control system failures resulting in control actions which would make the accident consequences more severe than presently analyzed.

Licensees were, however, in late 1979 requested to review the possibility of consequential control system failures which might exacerbate the effects of high energy line breaks and to adopt corrective action where needed to assure that the postulated events would be adequately mitigated.

Now, I intend to talk about that a little bit more when I try to summarize the things that have been done recently and the things that are under way which are related to this issue on control systems.

MR. EBERSOLE: Comment. I find it fascinating that we have a topic here, high energy line breaks, which ignored the more likely possibilities that these manifolded systems could be lost, as well as having high energy line breaks.

It seems to me that those should have been examined coincidentally and if they haven't, that should be done now.

MR. KERR: That is not a question, that is a comment. Please continue.

MR. ROSSI: Accidents could conceivably cause control system failures by creating a harsh environment in the area of the control equipment, or by physically damaging the control equipment. Also, by the mechanism that you pointed out, if you have manifold systems feeding detectors, an accident involving the manifold.

Also, control equipment damage and an accident could presumably have a common cause through some event such as a fire. It is again emphasized that the primary issue is not whether the trip or safety system action would be defeated by induced control system failures, but whether the control system failures would cause the accident to proceed in a manner potentially more severe than currently analyzed, and whether control system failures might confuse the operator such that he takes improper actions which worsen the accident.

This is very similar to the discussion which we had on anticipated operational occurrences.

Again, our reviews have looked carefully at control system failures that might in some way prevent a trip or prevent safety system actuation, and we have tried to eliminate all of those kinds of situations in a systematic way.

We have not been as systematic in looking at consequential control system failures which might simply make the accident proceed at a faster rate or in a way where the analysis is not conservative.

MR. EBERSOLE: A case in point. Would you be the party that would analyze the design of the control rod drive, supply and exhaust lines in BWRs to confirm in fact that a major LOCA(?) will not pinch out the flows of the discharge pipe and so prevent the insertion of the rods to the point it will go sub-critical when it is reflooded with cold, clean water?

MR. ROSSI: Faust, maybe you can answer that, I don't know.

MR. KERR: Well, you would know whether you would be the one tc review it, or not, which is what he asked.

MR. EBERSOLE: If you are not, who would?

MR. ROSA: Would you repeat the question?

MR. EBERSOLE: Faust, you know the control rod drives on many BWRs are segregated into quadrants wherein the tubes for supply and exhaust are located in the quadrants of the reactor and in fact they control quadrants.

These lines permeate the primary coolant precisely in the areas where you would expect immense mechanical damage as the result of a LOCA, that damage extending to closure of the discharge tubes, or pinch-off, or certain effects to the extent you could not insert rods subsequent to the LOCA.

When you have a BWR LOCA you do not flood, reflood, with borated fluid, unfortunately, you would reflood with cold, clean water, and you would never go sub-critical if a few of these rods stayed out.

That mechanical impact on control safety systems unfortunately is so intertwined between mechanical engineers and safety analysts that is has just simply been laying there for a long time and there has never been any conclusive settlement of the argument as to whether this could occur.

MR. KERR: Let me make sure, what is the question?

MR. ROSSI: That is really a safety system question.

MR. KERR: Are you asking whether this is reviewed at all, or whether this particular branch reviews it?

MR. EBERSOLE: How is it reviewed? Has it been reviewed, is it concluded?

MR. KERR: OK, the question is, has that issue been reviewed.

MR. ROSA: As far as I know, it has not.

MR. KERR: Thank you.

MR. ROSSI: Accidents or limiting faults are the most severe events analyzed for a nuclear power plant. As such, they in many cases would proceed on a time scale such that it is unlikely that control system malfunctions could significantly decrease the margin to core damage limits at the time of reactor trip or increase the amount of residual heat from those assumed in current analyses.

A trip is likely to occur before any control action can appreciably change any of the variables affecting either margin to core damage limits, or residual heat.

Finally, I would like to briefly consider the effects of control system failures on operator actions. Again, we have looked at the equipment that is required to maintain the plant in a safe shutdown condition.

MR. KERR: Mr. Rossi, I apologize for interrupting, but it seems to me the statement you have just made appears on page 7 of Mr. Ross' memorandum.

MR. ROSSI: It is, yes.

MR. KERR: I note that Dr. Hanauer's comment in the memorandum of December 13 says - and I read from his comment - "No analysis I know of substantiates the discussion on the middle of page 7."

MR. ROSSI: There is no question that what is said on the middle of page 7 is an engineering judgment-type of statement that the big accidents proceed at a rate such that it is unlikely that control system malfunctions that might occur would appreciably affect the sequence, the rate of change of parameters during the accident.

We have not done analyses to verify that, that is correct. I agree with Mr. Hanauer's comment. I would hope that the wording in here, what I said, did not imply that we had done an analysis.

MR. KERR: It seems to me that indeed Mr. Hanauer goes on to say, "Not all severe accidents have in the past, a small-break LOCA is an example."

I personally think, and now I may be reading between his lines, that he is doing a little more than saying that there has not been any discussion that substantiates the discussion of this statement. I think he is saying he disagrees with it.

MR. ROSSI: There are certainly cases where consequential control system failures caused by the environment that might be created by the accident could be a problem. Another example is this high energy break thing that we were talking about before. I did not want to indicate that in all cases this was correct.

MR. KERR: Thank you.

MR. ROSSI: I am trying to give some flavor of what were the biggest things, the worst things that might happen. It is improbable that you are going to have significant effects. I am not trying to say that we have done analyses that show it can't occur because that is not the case.

In addition, recent emphasis on the availability of post-accident instrumentation will result in the initiation of additional NRC staff reviews to ensure that control system failures will not deprive the operator of information required to maintain the plant in a safe shutdown condition after any anticipated operational occurrence or accident.

Systematic evaluations of control system designs have not been performed to determine whether single failures, or single failure/event induced multiple control system failures could result in confusing or incorrect operator information, or in a transient not bounded by current analyses with the plant at shutdown during plant heatup or cooldown, following plant trips, or following actuation of engineered safeguard systems.

Single failures or events which might conceivably induce multiple control system failures could presumably include events such as loss of power supply, fire, or earthquake.

Now, the consensus judgment of the NRC staff is that the risk associated with control system failures is not sufficient to require immediate corrective actions. However, to provide added assurance that the current licensing practices which I have described here this morning are adequate, the following actions are under way:

The Commissioners, as I am sure you know, have now approved the "Safety Implications of Control Systems" as an Unresolved Safety Issue.

B&W has completed a failure modes and effects analysis and review of operating experience for their Integrated Control System and reported the results in a report entitled, "Integrated Control System Reliability Analysis."

Consultants from the Oak Ridge National Laboratory have reviewed the B&W report and concluded that although the ICS and related control systems could be improved, the ICS itself has proven to have a low failure rate and does not appear to precipitate a significant number of plant upsets.

Failure statistics revealed that only approximately six of 162 hardware malfunctions resulted in reactor trip. Oak Ridge further concluded that the B&W analysis shows that anticipated failures of and within the ICS are adequately mitigated by the plant safety systems and that many potential failures would be mitigated by cross-checking features within the control system without even challenging the plant safety systems.

Oak Ridge agreed with B&W conclusions regarding control system improvements which could be made to improve overall plant performance. Licensees with B&W plants have been requested to evaluate the B&W recommendations and to report their follow-up actions. The licensee responses are currently being reviewed.

In September of 1979, all licensees were asked to review the possibility of consequential control system failures which could exacerbate the effects of high energy line breaks and to identify appropriate actions where needed to assure that the postulated events would be adequately mitigated.

The review was requested as a result of postulated scenarios involving consequential control system failures identified by Westinghouse and submitted to the NRC by Public Service Electric and Gas. All Licensees responded to the request and the responses were screened.

On the basis of the review, no specific event leading to unacceptable consequences was identified and, in general, control equipment locations were such that consequential failures would be unlikely. Some licensees, however, did make changes to operating procedures to include the possibility of control failures. In-depth, systematic reviews were not made by the NRC staff, but considerable reliance was placed on the reviews of the licensees made as a result of our requests to them.

A bulletin has been issued and a supplement prepared for issue to licensees requesting actions to ensure the adequacy of plant procedures for accomplishing shutdown upon loss of power to any electrical bus supplying power for instrument and controls.

Licensees have been specifically asked to address changes of state of plant equipment and automatic control system actions resulting from loss of instrument bus power. Some licensees have taken corrective action, including hardware changes and revised procedures to assure that single failures of power supplies will not simultaneously cause transients and failure of instrumentation required to mitigate these transients. That, I think, addresses one of the specific concerns you brought up this morning.

The Office of Standards Development is coordinating efforts with the IEEE to establish design criteria for systems that are important to safety which are not covered by, and do not need to meet all of the rigorous standards for safety grade equipment but nevertheless are sufficiently important to safety to perhaps be included in the NRC review process.

Emphasis on the availability of post-accident instrumentation and the preparation of Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident" will result in the initiation of additional NRC staff reviews to ensure that control system failures cannot deprive the operator of information required to maintain the plant in a safe shut-down condition after any anticipated operational occurrence or after any accident.

Indian Point 3 has been asked to do a Systems Interaction Study in which control system problems will be one aspect. The contractor for this study is Ebasco, and a commitment has been made to receive a plant for the study by mid February.

Standard Review Plan Section 7.7 calls for staff reviews to assure that failures of control systems will not impair the capability of the protection system in any significant manner or cause plant conditions more severe than those for which the plant safety systems are designed.

The staff has pursued these reviews primarily to ensure that electrical interconnections between protection systems and control systems are implemented such that failures in control system equipment cannot impair the operation of protection system equipment.

Recently, the Instrumentation and Control Systems Branch has drafted for internal comments questions that might be asked during the review of license applications to further address the content of Section 7.7. The licensees would be required to evaluate the effects of single failures and single failure or event-induced multiple failures on the indication, manual control, and automatic control for key plant parameters and equipment.

The responses to the questions, along with the actions discussed above,will provide additional insight in establishing a more systematic methodology for assessing the impact of control system failures on plant safety.

That brings to conclusion the prepared presentation that I had to make this morning.

MR. KERR: Thank you, Mr. Rossi.

Are there questions? Nobody has a question? On your presentation, Mr. Rossi, I have some questions.

In your presentation you gave us some idea of a staff philosophy about this review. I wanted to ask if you feel there has been any significant change in this philosophy, say, over the past couple of years. As I listened, I could not tell if there had been. It seems to me one could have said about what you said two or three years ago.

MR. ROSSI: I think it is a fair statement to say that there has not been a significant change in philosophy. I think that events over the last two years, however, have led us to look into the areas I summarized there at the end in more detail to try to review whether there is a need for a change in philosophy. That has been the primary effect of the events in the last two years, to kind of instigate additional probing into areas which would tell us whether what we are doing is the right thing.

MR. KERR: One of the statements you made, for example, was that you had some kind of an incident and there were no serious undiscovered control system problems because if there were they would have been uncovered in operating experience by now.

MR. ROSSI: That was mainly directed, that comment, at the anticipated operational occurrences because the probability of an accident would be so low that I don't think we could depend on operating experience for that.

MR. KERR: Well, anticipated operational occurrences can develop into accidents. I am thinking of one where it seems to me it did. It seems to me you could have made the statement with almost the same number of reactor years experience for TMI II.

Now, I don't know whether TMI II has changed your attitude towards the possible seriousness of interactions, or the seriousness of nonreliability of control systems or not. It seems to me there has been some impact on some people's thinking.

MR. ROSSI: Well, I would say that TMI II and the action plan that was developed as a result of it, has kind of re-emphasized a lot of things that were going on. Like in the area of systems interaction, for example, I think there has been and will be additional emphasis there; and perhaps looking at whether there ought to be additional things that are now non-safety grade brought somehow into the licensing process.

I think Three Mile Island may have put a greater emphasis on that, too. So, I would see Three Mile Island primarily as just having strengthened the emphasis on some of the things that were already being considered. It may have changed some priorities somewhat, too.

MR. KERR: Mr. Ebersole?

MR. EBERSOLE: I believe I heard you say that some operators and applicants have elected, not particularly under pressure from NRC, to change those regimens where a power supply failure coincidentally affected control and safety systems.

What bothers me a little bit is that they had to elect to do that of their own accord. That there evidently was no pressure on the part of NRC to have to, in the first place.

MR. ROSA: I don't think it is fair to say that they elected to do that without any pressure from the NRC. I think every time an incident occurs and we can mechanistically identify a case like this, that not only the applicant involved or the licensee involved, but also the other licensees are notified and urged to review and make appropriate corrections.

MR. EBERSOLE: Well, what led me into it Faust, was the impression that some of these have done it, implying that others have not bothered to do so.

MR. ROSSI: Well, we are still in the process of reviewing responses.

MR. EBERSOLE: That is in process now.

MR. ROSSI: That is under way now.

MR. EBERSOLE: So, we are at some point in-between.

MR. ROSSI: Yes. Most of these actions that I summarized here at the end are open to some degree - I would say every case.

MR. EBERSOLE: Is there a closure time on this sort of thing, is it "dribbling" along?

MR. KERR: Please, say it is not "dribbling" along.

(Laughter.)

MR. ROSA: No, it is not "dribbling" along. I was going to say that every significant incident of this type is covered by at least a bulletin which specifies a due date for the response and resolution.

MR. EBERSOLE: Thank you.

MR. KERR: I think I understand what you are driving at. But let me say that I am delighted that some people chose to make safety improvements voluntarily.

MR. EBERSOLE: Right.

MR. KERR: I would hope that not all safety improvements would have to be under NRC demand.

MR. EBERSOLE: I would second that.

MR. KERR: With all due respect to NRC, they can't make reactors safe by themselves.

MR. EBERSOLE: Correct, I will agree to that.

MR. KERR: Mr. Basedekas, I know you had some concerns in this area that has been written about and spoken about in other forums. I want to ask you at this point, are there any comments you would like to make?

MR. BASEDEKAS: I just want to briefly comment on some of the statements made this morning.

I do know you have some of the documents in which I have discussed our concern before. I will not repeat what is there. However, I will beg you to read them, if you have not already. I gather that at least in your files here you have hopefully copies of the letters to Dr. Ahearne, one to Mr. Udall, one to Tom Merley.

Let me start by saying that I agree with Steve Hanauer's comments, generally speaking, the letter that you mentioned earlier, Mr. Chairman.

One of the things that I talked to Steve about was the statement of Mr. Parker where he states that it is true that the direction of a power plant will reduce the reduction of consequences, but not in probability. I think one should attempt to focus on what was in his mind, anyway.

What probability he has in his mind on failures of control systems that may shake the sequence, not necessarily the probability of a sequence, one that may be completed in some unsafe point. The theory is, given a set initiator and considering the progression was set in sequence from a one-hundred percent power level versus a progression from, let us say, something like 65 percent power level, then the end result, the end state of the plant in one case may be unsafe while the other might survive. That is a point that he consistently made.

I think another point you made yourself as you went along. As you know, control systems are qualified, and if the roof falls down, then we are in trouble. So, the effort to develop criteria for design installation of control systems is very important. So is the effort that is presently under way by the IEEE working group to classify safety systems.

Notably, you might be interested that it is specifically decided to exclude control systems. Now, you take it from there.

Another point I wanted to make was that licensee event reports are part of the requirements by the utilities and do not include control system failures unless this has resulted in some sort of a challenge to the safety system, like safety checks. So, the data varies to date, it is not complete, I believe, and important requirements reflect that.

I believe that the discussion to some degree this morning reflected the long-held philosophical approach to this problem by the staff which has been centered around what has been referred to as events of occurrences which are more benign events, which they by definition are. I think it might have been either explicit or implicit and to that respect it should be tempered with the understanding that, as you pointed out --

Another point I want to make is something that is obvious, but it is prudent at some times to repeat it, and that is that control systems by themselves don't mean anything unless one includes the dynamic processes.

I think the statement made by Mr. Rossi that in the judgment of the staff, that the risk as perceived by the staff that may be attributed to control system failures and other issues as to non-safety conditions do not warrent immediate action. That is something that I disagree with, and I have made that clear for some time.

With respect to the performance by B&W, the analysis, certainly, it was a step - I thought then and I still do - a step in the right direction. But it is only one step, and a rather short step. Not only did it stop there with respect to the B&W effort, but also, I believe, it was not extended to include the other vendors that may have the same problems. There may be different problems as far as design, their plant scope, but I think the same problems do exist for all the plants.

I hope this effort, hopefully at least in my mind, is intended to prevent accidents and not having to deal on a crisis basis where we have then to explain after it happens. That this is something we will try to improve on.

Also, with respect to the purpose of this question, I believe the control system centrally is important, but it has to be looked at in the context of how the plant dynamics will affect the progression of an accident sequence and hence the possibility that it may affect the probability of accident sequences even if the viability of the system is high in its electrical or mechanical sense.

To put it another way by an example, assume, for instance there is a design deficiency, an inherent design problem with the control system, that will have a tendency, by design, to drive the plant to a condition that will be less safe. It makes the probability that it will perform in an undesired function more likely. This has to be addressed, as I said, with design criteria.

10:25
Riley
fls

While I notice the candid remark in response to your question, Mr. Chairman, there has been no change in philosophy. I was hopeful that it was in the process of taking place, and I still do hope it is.

I think the statement the Staff has made that we are still sticking to the old way of thinking, of approaching this problem, has changed somewhat. At least, that has been my perception.

I hope I misunderstood their comment.

I think the perception in some quarters -- and that includes some quarters in this agency and certain of the industry and this government -- it appears that the TMI-2 accident has served as what you may describe as a proof test that the system worked. Nobody was killed.

I think this is a very dangerous position to take and base, you know, whatever future actions we may have to take on this type of interpretation of what the TMI-2 accident really means.

Here specific rumors abounded, and were stated to Congress that, you know, what we have to worry about? The system worked. I think this is unfortunate, and I hope it can change when people like you will find it prudent and appropriate to speak their minds a little more openly than we have in the past.

I think the comments that were made early, as you correctly pointed to, Mr. Ebersole, were out of the reactivity control systems and the inferences that you make about those statements should not be extended to include the control systems and how failures of those systems will be reflected on the primary.

And I think another example for which perhaps you might find it appropriate to request a special briefing from the Research Office will be consideration of the fact that a failure or perhaps multiple failures, depending on the particular design of a PWR on the secondary side of the main feedwater, in particular, control system may result in large main feedwater flow after -- for something like 10 or 15 minutes. This, in conjunction with other things, such as the ECCS on the primary side and not turning that off, may result in rapid and substantial loss of the primary, with the likelihood that the pressure vessel will fail.

MR. KERR: I should emphasize that we do not plan to finish this discussion today, and I would prefer, if possible, to sort of put emphasis on detailed questions at later meetings. And thank you for those comments.

Let me ask the Staff, if I can -- and, incidentally, some of the questions that are raised today I won't necessarily expect an answer to today, but I think it is important that we begin exploring some of these questions.

How do you interpret Mr. Udall's question? I mean you have had to deal with it longer than we have, so you must have come to some local interpretation.

I cannot tell for certain whether he is saying -- if you don't try to read between the lines, the letter seems to say, "Tell us how the Staff reached the conclusion they reached."

Now I cannot quite believe that is all he is saying, but maybe it is. I rather assume that he is saying, "Go over the information available to you and to the Staff and see if you were to reach the same conclusion." That is sort of my interpretation of his question.

Are you willing to comment on how you view his question? Because I think the attitude that one takes toward this question has some influence on how we explore this, and in a very simplified way, it determines whether I put emphasis on trying to crawl inside the minds of the NRC Staff which I am sure I am not capable of doing. Or whether we put emphasis on trying to make certain that we understand the information and philosophy on which you based your decision, and then trying to decide whether we agree with it.

Do you understand the question? It's a hazy question, because I am a bit puzzled myself as to the question being raised.

MR. ROSA: As I said earlier -- well, at the beginning of this session, I am relatively new in this area. Speaking for myself, therefore, with a somewhat limited detailed background, I would agree with your interpretation of the question.

Now, having said that, I am going to ask Ernie Rossi here to say -- to express his opinion on that, since he has been involved in this since it has been assigned to ISC.

MR. ROSSI: Well, I would assume that what Mr. Udall would like to know is whether you feel that there is some immediate problem that would necessitate a change in priorities that we have given to this particular area from what they are now; whether there is any problem that is of a nature that would require some sort of action on operating plants in the short time-scale; and in addition, as to whether we have defined the problem, and are approaching the problem in the correct manner.

Those are the issues that I would assume that he would want your advice on.

MR. KERR: Well, that is, I think, my own interpretation of what I think he means.

Now, let me see if I understand what the Staff has done, because it seems to me that it has done a number of things since TMI-2, even though it may not have changed its basic philosophy.

One of the more significant actions, it seems to me, is a designation of control system reliability as an unresolved safety issue.

It is my understanding that that is now formally an unresolved safety issue. That's correct, is it not, from the publications I have seen?

Karl, we probably ought to get a mike if we can. Because these words are being recorded.

MR. KNIEL: My name is Karl Kniel and I am Chief of the Generic Issues Branch, and the answer to the question is yes. The Commission approved safety indications of control systems as an unresolved safety issue, in the memo from the Secretariat.

MR. KERR: The title given to it is --

MR. KNIEL: The title that we have given to it and we have adopted is "Safety Implications of the Control System." I think that title appropriately envelops --

MR. KERR: I'm not trying to disagree with the title. I just want to make sure that I have it correct, because one of the things we are going to have to do is write an early response, and I want to use the right words.

MR. KNIEL: "Safety Implications of the Control Systems."

We did get a memo from the Secretariat where the Commission has agreed that that should be an unresolved safety issue.

MR. KERR: Now as I understand it, having designated something as an unresolved safety issue gives it some sort of priority? I'm not sure I know what, but it does put it very near the head of some list, in terms of resource allocation, in terms of scheduling, these kinds of things.

Can you give me some insight into generally what this implies?

MR. KNIEL: Yes, sir. Organizationally it puts the management of the resolution of this now in the Generic Issues Branch, where the other unresolved safety issues are managed. In terms of priority, the Director of NRR has listed unresolved safety issues third in priority; after problems with operating plants and after near-term OLs, comes unresolved safety issues.

So it has a fairly good standing in terms of priority of effort.

MR. KERR: Since this is now an unresolved safety issue and it has gone into the generic items, what was the terminology? Branch?

MR. KNIEL: Generic Issues Branch.

MR. KERR: Generic Issues Branch. What happens to it then?

MR. KNIEL: Well, we will be appointing a task manager and we will be writing an action plan.

MR. KERR: When will you be appointing a manager?

MR. KNIEL: We are in the process of doing that right now.

MR. KERR: So by next week, this time next week, there will be a task manager, probably? I'm not trying to tie you down to something.

MR. KNIEL: A week or two or something like that, yeah.

MR. KERR: So, for example, by the February meeting, if we should write a letter and want to say that, we could probably say that a task manager had been appointed?

MR. KNIEL: Yes, I think you probably could.

MR. KERR: Okay.

MR. LIPINSKI: Mr. Chairman, with that title, there is a paragraph of description that goes as to how you view the problem.

MR. KERR: I beg your pardon?

MR. LIPINSKI: He only gave us a single title for the generic issue, but there's usually a paragraph of description that goes with each one of those titles.

MR. KNIEL: That's correct. We have provided a paragraph of the description.

MR. KERR: We unquestionably have that somewhere, Walt. I just want to know how to find it.

MR. LIPINSKI: At this point I was interested in seeing how they view this as a generic issue, as to what the problem is.

MR. KERR: Do you have that description, or does someone have it?

MR. KNIEL: Yes, I have it. We did discuss this in our memo to the Commission that we issued, I think, in September. I don't happen to have that memo with us.

MR. KERR: We read all those very carefully, but don't memorize them.

MR. KNIEL: We did write a one-paragraph summary of this issue for the annual report, the NRC annual report, and I can read that to you.

MR. KERR: Please.

MR. KNIEL: "Safety Implications of Control Systems," and we have designated them as Task A-47.

"This issue concerns the potential for accidents or transients being made more severe as a result of control system failures or mal- functions.

"These failures or malfunctions may occur independently or as a result of the accident or transient under consideration and would be in addition to any control system failure that may have initiated the event. Although it is generally believed that control system failurrs are not likely to result in loss of safety functions which could lead to serious events or result in conditions that safety systems are not able to cope with, in-depth studies have not been performed to support this belief. The potential for an accident that would affect a particular control system -- and the effects of the control system failures -- will differ from plant to plant. Therefore, it is not likely that it will be possible to develop generic answers to these concerns, but rather plant-specific reviews will be required. The purpose of this Unresolved Safety Issue is to define generic criteria that may be used for plant-specific reviews. A specific subtask of this issue will be to study the steam generator overfill transient in PWRs and the reactor overfill transient in BWRs to determine and define the need for preventive and/or mitigating design measures to accommodate this transient."

You may be aware -- I think there has been some reference to the overfill transient here today. There has been a lot of discussion on this particular transient. I think it is representative of a control system failure that we have not rigorously looked at, that could have potential consequences, and because of the specific discussions that we have had with the Commission, and with Carl Michaelson's group, we agreed that it should be specifically called out in this task as something we should address.

MR. KERR: Okay.

MR. LIPINSKI: Mr. Chairman, would it be possible to get a copy of that and study it?

MR. KERR: I can say unequivocally that it would be possible.

MR. LIPINSKI: Thank you.

MR. EBERSOLE: (Inaudible.)

MR. KNIEL: The overfill transient will specifically be a subtask in the way we see it, the way we are going to plan it, and we would attempt to generate a resolution of the subtask on a more rapid timescale than our handling of the entire problem.

MR. EBERSOLE: When would that be?

MR. KNIEL: We have got to sit down, we have got to write an action plan, and the action plan includes what are we going to do, including what are we going to do on this particular -- how are we going to study it. And after we decide what we are going to do and what resources we have to do in terms of people and money, then we will write a schedule. When we have that schedule, we will know when it is going to complete.

MR. EBERSOLE: It sounds kind of ponderous to me. Hasn't there been an awful lot of work done already on this matter?

MR. BASDEKAS: Some.

MR. KNIEL: The work that has been done, has been done in terms of --

MR. KERR: Excuse me. For my own understanding, are you talking about the overfill problem?

MR. EBERSOLE: The overfill problem particularly.

MR. KNIEL: Well, I don't have a specific schedule. I think enough work has been done so that we can see our way to a more rapid resolution of this particular issue within this unresolved safety issue, and we will specifically detail a schedule for resolution of this particular issue, irrespective of the total issue. But I do not have a schedule for that today.

MR. EBERSOLE: Thank you.

MR. KERR: Mr. Ray, I think you had your hand up.

MR. RAY: I had a question similar to Jesse's, but it was to the implications of the control systems. I wondered how its priority will rank with respect to other unresolved issues that are already on deck.

MR. KNIEL: When you say "unresolved safety issues," if you are comparing it to unresolved issues, I am sorry -- you used the word "unresolved issues." I used the word "unresolved safety issue" in a very specific sense.

These are the issues that the Commission has deliberately designated as issues of major importance for which we feel that there would probably be some fix required for operating plants in the long term, either procedural or hardware or some such kind of change.

There is a specific definition -- I don't have the definition with me -- of unresolved safety issue, but the unresolved safety issues have the highest priority in terms of generic issues, I think.

MR. KERR: My impression was, Mr. Ray was asking if you line up all the unresolved safety issues, where in the chain would this be? At the head of the list or the bottom of the list, or somewhere in the middle?

MR. RAY: That's right.

MR. KNIEL: If that is your question, we never have prioritized the unresolved safety issues. We give them about equal priority.

MR. RAY: But this is in that class?

MR. KNIEL: This is in that class. As I indicated earlier, the Commission has -- we have had a long dialogue with the Commission, with which the ACRS has participated. The ACRS happened to suggest this issue, and suggested certain features of it that we agreed with the ACRS that it should be an unresolved safety issue, and the Commission agreed, and it now is.

MR. KERR: Did that respond to your question, Jerry?

MR. RAY: It does, but it doesn't make me feel any happier about it.

MR. KERR: We cannot promise to make committee members happy at this meeting.

(Laughter.)

MR. KNIEL: There's no priority within the unresolved safety issue group. We had 17. We have added four. We have resolved quite a few of them, five or six of them now.

MR. RAY: Well, what determines what the date for action will be when you set up a schedule and so on? Is it that there are others already waiting in line for tickets and therefore they get preference?

MR. KNIEL: No.

MR. RAY: Well, is there a relative judgment at that time as to the relative importance of this issue as compared with others, so that you will put people on this one earlier than others?

MR. KNIEL: Most of the issues are in different areas. They don't compete with each other. They may compete with resources of the Staff in other areas, and I have indicated to you what the priority is there. The priority is operating plants, near-term operating license, and then unresolved safety issues, but they tend not to compete with each other. So I don't see a problem there.

MR. RAY: Well, might I interpret what you say? I get the impression from this statement what you are saying is you could very well work on this in parallel with working on other unresolved safety issues.

MR. KNIEL: That's absolutely correct.

MR. RAY: Therefore, just because it's coming aboard now, it's not going to suffer from the viewpoint of preference?

MR. KNIEL: That's correct.

MR. EBERSOLE: Mr. Chairman, it occurs to me to identify an issue as an unresolved safety issue may put it in a parking lane where it ought not to be. It ought to be subject to more vigorous --

MR. KERR: I remind you that this was done at the suggestion of the august body called the Advisory Committee on Reactor Safeguards.

MR. EBERSOLE: I wonder, however, if they realize that the end result of that might have been to put it in a parking lane?

MR. KERR: I'm sure they wouldn't have done it, if they had realized that.

MR. EBERSOLE: Is it in fact --

MR. KERR: If Mr. Kniel can be believed -- I have no reason to disbelieve him yet -- this has high priority. It gets a task manager, resource allocation, and even in spite of your remarks to this as being a ponderous process, he's getting underway.

MR. EBERSOLE: I heard all that, but I didn't hear anything material in it anywhere.

MR. BASDEKAS: Mr. Chairman?

MR. KERR: Yes, sir.

MR. BASDEKAS: I believe I should say something along this line that would indicate that the attention paid by the Staff is increasing in tangible ways, and I think as part of this additional attention, the Research Office will be undertaking a task in conjunction or perhaps in addition to what at this time at least --

MR. KERR: You mean we're going to get the Research Office mixed up in this, too?

MR. BASDEKAS: Yes, we are.

MR. KERR: Oh, god.

(Laughter.)

Go ahead. If I may be facetious.

MR. BASDEKAS: That's all right. Well, this same august body you referred to earlier suggested that we undertake such problem, so we are just proceeding on that directive, so to speak.

MR. KERR: Thank you.

Are there other questions? Mr. Lipinski?

MR. LIPINSKI: We have discussed what the NRC has done, but right after the TMI accident, I had provided information to the ACRS on the Canadian licensing procedures, because I had been exposed to them just prior to the accident. They take a more conservative approach, or they did at the time, with respect to the review of control systems, and Mr. Fraley evidently tried to get additional information, and somehow they are in some state of limbo where they have not issued their position as final gospel.

Consequently --

MR. KERR: The problem, Walt, is they don't have enough lawyers. The last time I talked to them, they had a staff of 70 engineers and only one and a half lawyers.

MR. LIPINSKI: I suspect the Germans may be more conservative, based on some information I have, but on control systems I have no specific information. I just wondered if the Staff had been looking at what happens with the control system reviews by other licensing agencies in other countries.

MR. KERR: Is that a question?

MR. LIPINSKI: Yes, it's a question for the Staff.

MR. ROSA: I can't answer that.

MR. KERR: But you could maybe find out for us, so that we could get some information on that at a subsequent meeting?

MR. ROSA: Yes, I can.

MR. LIPINSKI: Okay.

MR. KERR: Are there other questions from members of the subcommittee?

Mr. Kniel, if I chose to read between the lines of that explication of the unresolved safety issue, I could interpret it to mean that the Staff believes that the position it has taken, which is one of not looking very carefully -- not looking at detail -- don't let me use the word "carefully" -- not looking at the detail of the control system performance is the right one, and that this investigation is going to demonstrate that indeed it is the right approach.

Now I would have hoped, and indeed I still hope, that in the course of its investigation, the Staff would maintain an open mind and at least there might be some probability at the end of the study that a different approach could be recommended.

That's not a question. You can comment.

MR. KNIEL: The objective of making an unresolved safety issue is to take -- to start a fresh new look at the whole new problem without any preconceived --

MR. KERR: If you read that paragraph, I'm not sure that comes through, but maybe it's just my interpretation of English, which is not always good.

MR. KNIEL: I think part of your introductory comments -- the way I look at it, I think in many cases we have taken a detailed look. What we have not done, as the word has been used here fairly frequently this morning, i a systematic and rigorous --

MR. KERR: I'm accept systematic and rigorous.

MR. KNIEL: That s what we would like to do. The main reason I am down here this morning, with Paul Norian, who is the section leader of the branch, is to get some of the thinking of the subcommittee on how they view the problem, so that we can appropriately write an action plan that will cover the major features of the problem as viewed by those who have studied it.

MR. KERR: Now is there -- are you able to predict at this point with whatever uncertainty is necessary, when this action plan may come into existence?

I mean, for example, as the subcommittee chairman, I am predicting that it might take us six months to complete this review for Mr. Udall. The six months is sort of arbitrary, but is it likely that there will exist an action plan in final form at the end of that period? Or is it likely to exist two weeks from now, or what?

MR. KNIEL: I would like to have some kind of an action plan ready in about three months, but it may not have had the collegial review that it might take.

MR. KERR: What about the draft that starts the process? How soon is that likely to exist? I ask this for a very practical reason. I can't tell in that paragraph what you are going to do, and I may not be able to tell after I see the action plan, but I ought to have a better idea. It's fairly crucial to our comments to know how the Staff plans to go about this.

MR. KNIEL: I think it's going to take us three months to generate an action plan that you could get some real substance out of. We may have a draft at some time before that, and I would hope that after you read the action plan that you would then understand what it is we propose to do.

Certainly we would like to discuss our proposed action plan with the subcommittee.

MR. KERR: Mr. Ebersole?

MR. EBERSOLE: While you are generating the general action plan, is there any reason that you shouldn't take a few particular topics that appear to be of immediate interest, and also work on them?

MR. KNIEL: Yeah, we have already designated that one. Everybody has recognized, including the Commission --

MR. EBERSOLE: (Inaudible.)

MR. ROSSI: My understanding is that the Westinghouse plants have equipment installed in their control and protection system that shuts off the feedwater, and that they have looked rather extensively at the excessive feedwater transient.

MR. KERR: I would prefer that we not carry out that investigation here this morning. I am not saying that to downgrade the importance of the issue; I think it obviously is important.

What we ought to do is get you and Mr. Ebersole in a closet. In about 15 minutes we probably could solve the problem.

MR. LIPINSKI: Mr. Chairman, having looked at the paragraph on Task A-47, this addresses the consequences of these failures, but there is no reference to the frequency, and I think that is an important ingredient as to -- and this relates --

MR. KERR: I would hope this is not the Task Action Plan.

MR. LIPINSKI: Well, the reliability of the control system is directly related to the failure --

MR. KERR: It was apparent to me, as I listened, that nothing in here was said about reliability, and I was somewhat disappointed, but the action plan, of course, may be more complete.

It seems to me that one almost has to address the question of reliability at some point. Having addressed it, one may say, you know, forget it. But I don't see how one could ignore it.

MR. LIPINSKI: I don't think you can, because it's the challenger in terms of the failures as they occurred to cause these consequences.

MR. KERR: I'm going to declare a 10-minute break, and when we come back, we will continue this discussion.

(Recess.)

T.2

MR. KERR: May we reconvene?

Let me talk briefly about this draft letter that some of you have before you. This I put together for your persual as something that after your suggestions are incorporated could go to the Committee. I would guess at its February meeting the Committee will write a preliminary letter to Mr. Ahearne because I think the schedule for hearings is such that probably if the Committee is to write a letter, it has to be done in February, and would form sort of a progress report on what the

Committee is doing in response to Mr. Udall's letter.

I don't propose to read this to you, but let me highlight those things that I think it says.

First, in paragraph one, I am estimating a six-month schedule, without being entirely clear about when one starts counting time. But I think that is probably about a minimum.

And then in the second paragraph -- and I will read that -- we note in this letter I envision would go to Mr. Ahearne, but that protocol will have to be decided by the full Committee.

> "We note in Congressman Udall's letter of December 4, 1980 that reference is made" -- and I quote from the letter --"'to the Staff's rationale on which its recent judgments relating to control system failures are founded.' We interpret this to refer to, A, the Staff's recent designation" -- and here I find I have the wrong wording. I had called it control system reliability, and the correct nomenclature -- where are my notes -- is safety implications of control systems. -- ". . .the Staff's recent designation of safety implications of control systems as an unresolved safety issue; B, its consequent commitment to deal with this issue on a priority basis; C, its decision not

to modify the control systems, to derate, or to close down plants currently operating until further operation is developed."

This is simply my elaboration of what I think he means by the Staff's recent judgments. These, I guess, are a result of the judgments rather than the judgment.

Then there are a number of paragraphs in which I have pulled from previous ACRS letters some of the comments we made on this general issue, and finally in the last paragraph:

"We expect in the course of the next several months to review this issue of control system reliability in some detail and to report to you our conclusions and recommendations."

Now you notice in my draft I had sort of put emphasis on reliability rather than safety implications. Again -- well, I have probably said enough.

Do you have any initial comments on this wording or this approach?

MR. LIPINSKI: I have a comment on this part, on its decision not to modify the control systems. I would like to go back to classification of control systems in terms of manual and automatic systems. There are problems with the manual control systems that we encountered on Rancho Seco, Crystal River, where the panels went blank, and I would like to get the Staff's response as to whether the inclusion of the safety parameter display panel solves the problems that were encountered in some of these earlier incidents, and what the status of its safety parameter display panel is right now in terms of the licensing process.

MR. KERR: Do you understand the question?

MR. ROSA: I believe I do, and I can't answer it. I believe that it's the province of the Human Factors Engineering Group, and I don't believe they are represented here today.

MR. KERR: Well, do you know enough about it to know whether the existence of a safety parameter display panel is now required for operation of plants? I guess the answer is no, but --

(Staff conferring.)

MR. MATHIS: Bill, I think -- I am not familiar with the details of the action plan, but I think this has to be in place at some time in the near future. I don't remember a date.

MR. MORRIS: I may not be able to tell you the date, but I believe NUREG 696, the NUREG that establishes the SPDS, the offsite operations center, the data link, will cover this issue and what will be required. SPDS will be required, but I don't know the date.

I would say that would be the reference.

MR. KERR: I think you have a good point. I think what Dick and I need to do is to find out what the status of that is, and it may deserve some additional calling out in Part C.

I think it's a good point. Mr. Ebersole?

MR. EBERSOLE: I wonder if it would be appropriate to note that there may be control systems in place now which unknowingly are controlling safety functions that have never been given recognition as doing so, and we are waiting for them to malperform to reveal the fact that they are in fact controlling safety functions, and they have simply been working.

The case in point is the level control.

MR. KERR: Are you referring to something we should put in this letter?

MR. EBERSOLE: Uh-huh.

MR. KERR: In what part of it?

MR. EBERSOLE: There may be in the matter of upgrading reliability or improving the control system, if we find in fact the control systems have been serving in a safety capacity, and we never did know that.

MR. KERR: What I had assumed we would say in this letter -- and that is, of course, subject to the subcommittee and the Committee -- is in effect we think we understand the issue you are raising. Here are comments that ACRS has made in the past on the issue. We expect to begin a set of meetings which we will probably complete in about six months.

Now whether we should go further is sort of a matter of subcommittee recommendation or final Committee decision.

For example, it may be that we should say something about derating which has been one recommendation. That's another thing that might go into the draft that we either do or do not think derating of operating plants is desirable.

MR. EBERSOLE: The thought I was thinking about was we may find it not at all appropriate to upgrade the reliability control system. That's a commercial consideration. We might find, in fact, that what is now a control system really should have attached to it safety system overrides.

MR. KERR: My question really is, do we want to put that in this letter, or do we want to make certain that we explore that issue as we go along? Because we may want to comment on it later. What do you think?

MR. EBERSOLE: Well, the thing with this letter, I think -- here and there I thought it was -- it was limited to upgrading or improving control systems, not to identifying the significance of their control; but doing something other than that.

MR. KERR: Well, I interpreted Mr. Udall to be raising that question about whether control systems have been looked at in enough detail and whether the right decision has been made. And, of course, there are a number of implications. Control systems alone, or as they interact with safety systems. A number of issues.

MR. EBERSOLE: Okay, you want to leave it general. I have no objection.

MR. RAY: It should be general.

MR. KERR: That would be my recommendati n at that point, but this is the subcommittee --

MR. EPLER: Can I make a comment?

MR. KERR: Yes, sir.

MR. EPLER: This may be a little longer than you would like, but I feel compelled to point out that this is not a new problem, and let me discuss two ends of the spectrum.

One problem has been with s for many years, and has received a great deal of attention. That is interaction between the reactivity control system and the protection system.

Now, many years ago, it was realized that no matter how hard we tried, we could not protect against any control system failure or, that is, failure to perform, or limited performance, let us say. And I'll give you an example.

In the first reactor that was built after the war, it was necessary to withdraw rods to increase reactivity by 40 percent delta K over K, which was just about twice that of the modern BWR. That was a lot of reactivity. The modern BWR gets rods out at about 10 hours. This reactor got the rods out in 5 minutes. This was a high performance system, the like of which has never been seen since.

Now it had limitations. We realized that we would have to limit the performance of the control system to make sure that the capability of the protection system would not be exceeded, but that is not enough. There is the reactivity anomaly, something that happens that we cannot control. We can control the speed of the rod drives, but if some rod were to somehow, for example -- and this is one example -- pull a rod out of the core gradually and the control system would compensate for this, and then suddenly turn it loose and go, flop, back in at an uncontrolled rate, you have had a situation that cannot be controlled. Some idiot might put in a rubber bag in the core and connect it to an airline, blow it up till it breaks, and you've got it.

Now we don't think this is going to happen, but we have to say we can't handle it if it does. That's a limitation we just have to say there's nothing we can do about it, and we hope the containment works.

Now, that's one end of the spectrum.

Now, the other end of the spectrum, we have had a great deal of discussion of separation of control and protection, and we have handled this exhaustively in the reactivity control level, but we don't have a separate system for protection in the heat removal area. We are using general purpose plant systems. You cannot talk about separation of something you haven't got.

Now this is a bit of an embarrassment, but I just learned yesterday from Gordon Edison that he is indeed working on the criteria and design of a dedicated system for heat removal that will permit us to have separation between plant and general purpose systems or nonsafety systems and a dedicated protection system.

He has two questions, I discover:

One question is, he is not sure how he can apply this is backfitting. And that requires considerable work.

The other question is most interesting. He doesn't know how he is going to sell it to anybody. And Mr. Udall, let me assure you that we are working on this problem and we will fix it, we hope, but we will not be required to review all of these nonsafety systems so intensively, because we think we will be able to have in some time a system of protection that will take care of these problems.

MR. KERR: Now are you suggesting that something like this should go in a letter?

MR. EPLER: At some point I would hope so.

MR. KERR: This letter?

MR. EPLER: I'm not recommending it, just calling it to your attention.

MR. KERR: Mr. Lipinski?

MR. LIPINSKI: I don't think the dedicated heat removal solves all problems, because you can still have core damage, and then remove the heat after the fact. But I would like to return to Mr. Ebersole's earlier thought on modification of systems that were not given the importance that they deserved, and namely the one is the pressurizer heater control.

MR. KERR: What I would like to do, if I can, is discuss the draft of this letter and finish with that.

MR. LIPINSKI: Again it relates to its decision not to modify control systems in Part C, because I think a bulletin and order went out, stating that the pressurizer heater controls had to be modified and a bank of heaters has to be in the diesel emergency power, because there was no requirement, and at one point --

MR. KERR: You're saying we should call attention to the fact that some modifications have been made?

MR. LIPINSKI: I would like to get the Staff's comment on that, as to whether that was amended or changed to a control system.

MR. ROSA: That was one of the lessons learned which the Power Systems Branch has been applying and has already been applied to operating plants.

MR. KERR: So we need to put in some "such-ases" and that would be a "such-as."

MR. LIPINSKI: That would be one, that an already-amended control has taken place -- control change.

MR. EBERSOLE: I might mention that that is a classical case where you can fix the control system for that sort of thing and still not look at the driving functions or the reliability of the ultimate process and find you have fixed the control system. But the receptor for that control impulse is not going to work.

MR. LIPINSKI: We haven't fixed it from a reliability standpoint, because we see the need for power, but there is not a specification that says it's got to be single failure proof, because the controller that's calling this is not a safety-grade controller as to what the reliability of that total system is.

MR. EBERSOLE: For instance, if you fixed and then added reliable parts to pressurizer heaters, you would find that the in situ installation of those are not environmentally qualified, anyway.

MR. ROSA: May I clarify that the Lessons Learned only required the capability to connect the pressurizer heaters' one bank and their controls to the safety busses.

MR. EBERSOLE: It did not require they work?

MR. ROSA: It did not require the heaters or their controls to be safety-grade.

MR. KERR: What is the status of control of the PORVs now? Does it have to be safety-grade or is it non-safety-grade? I will accept that "I don't know," provided we can find out.

I am talking now about the control of the PORV.

MR. ROSA: I don't believe the controls are now safety-grade.

MR. EBERSOLE: No, they are not.

MR. ROSA: They are now connected to a safety-grade power supply.

MR. EBERSOLE: Okay. But the controls themselves -- for that matter, neither are the PORVs themselves.

MR. ROSA: And the PORVs also are connected to a safety-grade power supply. There has to be a separate power supply from the block valve.

MR. EBERSOLE: In a way this tends to mislead people. When you say I have got this great high quality system connected to a lousy device which doesn't work, anyway.

MR. ROSA: If you will read the Staff's testimony on the Three Mile Island 1 restart hearing, you will find that there is justification for not making it safety-grade.

MR. KERR: These are all very important issues, but I want to talk about this letter, if I can.

Are there other suggestions you have for what should go in a very preliminary letter?

MR. MATHIS: Well, Bill, just one comment specific on the letter. On Item C, which we were just discussing, where you talk about modified control systems or derate, that really applies to Browns Ferry 3 incident, doesn't it? This basically --

MR. KERR: Mr. Basdekas has recommended derating all operating power plants until the control systems are fixed.

MR. BASDEKAS: As well as other --

MR. KERR: Now the Staff has decided that it does not want to recommend derating. That's the reason I put that in there. We may again take it out, put it in, whatever. It's also possible that the Committee would want -- I mean since Mr. Udall's letter refers to opinions of senior staff that disagree with the consensus, I assume that's one of the things to which he is referring, and so I thought it was appropriate to comment that that was one of the things he was referring to.

Now does the subcommittee or do the consultants think that the full Committee ought to comment in this letter on whether it thinks immediate derating is or is not appropriate?

MR. RAY: I think it's an appropriate comment. I think it should be in there.

MR. EPLER: Appropriate or inappropriate?

MR. RAY: No, appropriate. Because it was said in Ahearne's letter, with which he was not satisfied.

MR. KERR: Any other comments?

MR. EBERSOLE: Well, derating is an expensive way to enlist industry's assistance in this problem. That's the main thing, I think. It may be too expensive.

MR. KERR: Industry assistance is not all that is required, just because the Staff doesn't have a position, either, at this point, and industry wouldn't know what to do.

MR. EBERSOLE: Well, I think industry would find they have initiative.

MR. KERR: They cannot change things and get approval for them without Staff approval.

MR. RAY: Industry is not going to volunteer deration of their equipment.

MR. KERR: No, but Jesse says if you derate, then industry will do something, and that's a very good idea, provided industry knows what to do.

MR. EBERSOLE: Industry claims they know what to do. You hear endlessly that we shouldn't be -- what's that great word we have? -- prescriptive.

MR. KERR: Jesse, I'm sorry, but industry has to have approval of the NRC to do almost anything.

MR. EPLER: Mr. Chairman, could I support your position with this comment?

In the ATWS matter, which we have had with us for quite a long time, you have pointed out that we mustn't rush precipitously into changes, because we might make situations worse.

Now if we blackmail the industry into doing something by shutting these reactors half down, we will be doing something precipitously, and I think it would be not in the direction of increasing safety. So I would say let' .o these things deliberately.

MR. EBERSOLE: I think that's right.

MR. RAY: I support Ep here, and I also have a thought that if we were to take punitive action, if you will, and force a deration of plants that are operating today, what are we chastising them for? They haven't been told to make any changes in their designs for control systems and so on. So if we imply that because certain things haven't been done, you have got to derate to 60 percent --

MR. KERR: Yes, but there is another issue which we haven't discussed, and it seems to me it has to enter into this, and that is even though they don't know what to do and we don't know what to do, if we think that this issue is a serious safety issue, and that safety could be enhanced significantly by derating, then I think we ought to recommend derating.

MR. RAY: That is something else, though. I am addressing Jesse's thought that deration might be a good motivating influence on them to make changes.

MR. KERR: Okay. Good point.

MR. RAY: I think the tone of this letter and its contents serves the purpose very well. I just have a thought -- its'a small point -- I have some small editorials, but you can take them without discussing them here and taking the time to do it.

But at the top of page 2, where we refer to an intention of one of the subcommittees of ACRS to pursue the cascading chain of failures and control subject, if any action has been taken in this respect on this item, I think it would be well to record it.

MR. KERR: I do, too. That is something I need to investigate. I think the subcommittee has perhaps discussed it, but that is a good point, Jerry.

Would you make a note of that, Dick?

Anything else?

Okay, I think I detect a consensus that at least the subcommittee would not recommend derating at this point, and I will include this consensus in my report.

MR. RAY: I certainly express that point very definitely.

MR. EBERSOLE: I would also say this doesn't mean this can be handled on a relaxed basis, and that derating implies we can go on forever like we have on ATWS in fixing this matter.

MR. KERR: Do you think the six-month schedule is too short?

MR. EBERSOLE: That sounds fair to me.

MR. KERR: Okay.

MR. RAY: Well, I would just like to add a little bit of pressure to this thought. I am not recommending derating. If you were to recommend derating, Mr. Udall would have more problems among the Congressmen in the states that were affected than he has with these letters from the Commission, and I don't think you would be helping him a damn bit.

MR. BASDEKAS: Mr. Chairman, can I talk on a little point here?

MR. KERR: If it's a little point.

MR. BASDEKAS: I think we should advise the Congress on technical matters, not political views.

MR. KERR: Mr. Gilinsky has also commented on things that this Committee could comment on. I have found in the past that this Committee feels free to comment on almost anything it wants to comment on.

MR. RAY: I agree with this last thought, Bill, and that is my --

MR. KERR: That doesn't mean it should.

MR. RAY: That is my intention, and if isn't appreciated or others feel to the contrary, I would be willing to --

MR. BASDEKAS: I am speaking for myself, but I believe that technical matters should be --

pu2

MR. KERR: I would say safety matters, and that's not really quite the same thing, I think.

MR. LIPINSKI: After TMI, B&W was asked to do a failure modes-and-effects safety analysis for their control systems, but none of the other vendors were ever asked to do an equivalent exercise, and this would not be the responsibility of the Staff, but it would be the responsibility of the vendor to provide what he thinks the failure modes-and-effects analysis amounts to, and that immediately signals problem areas.

MR. KERR: Are you suggesting that we put something about this in the letter, or --

MR. LIPINSKI: I am projecting it as a thought right now, because we have looked at this Task Action Plan --

MR. KERR: No, I'm trying to --

MR. LIPINSKI: I want to give my thought openly, and then the ACRS can consider how they want to handle the thought. But we already know what B&W's shortcomings are, based on their failure modes-and-effects analysis, but we don't know the others'.

MR. KERR: My question is, do you think in this letter we ought to suggest that the Staff require a failure modes-and-effects analysis of all vendors?

MR. LIPINSKI: Yes, this would be my proposal, because this work can be done on a rather short-term time basis while the Staff is gearing up on some of the other aspects of the control systems interactions. Because this is simply a tabular presentation of, as you say, -- run to the limit and have the thing go full speed, full value, and then like a PORV sticks open or something like this, what are the consequences. If there is a power supply somewhere in someone else's system, and it goes out, it takes off in four or five different directions, and the wrong direction --

MR. KERR: I will report your recommendation to the Committee. I don't think, personally, that should go in this letter.

MR. LIPINSKI: It could go through a different path, but --

MR. KERR: I will report that as a recommendation.

Are there other comments on this letter?

And keep in mind that this is really a very drafty draft. It's something that will go to the Committee. The Committee may want to address both the ATWS issue and the control system issue in one letter, and probably will. So I think this is just -- okay. I think there have been a good many helpful suggestions here, and Dick and I will try to modify the draft accordingly and give it to the Committee.

MR. EBERSOLE: Bill, there is a theme in this draft that I would like to ask you to think about from time to time here. I see it refers to reliability assessments and so forth. Isn't what we are really after not reliability assessments? It's what is their potential for creating safety problems. Reliability assessments to me means how frequently they are going to create some kind of a problem.

MR. KERR: Well, Jesse, I had thought that the issue was the Staff's conclusion that one did not need to make a reliability assessment of the control system.

MR. EBERSOLE: One needs to make an assessment of its ultimate competence to cause trouble.

MR. KERR: I am not suggesting this letter is going to solve all the problems that exist. It may not solve any. My understanding was that the issue about which Mr. Udall was concerned was the current position of the Staff which he interpreted to be one of not looking at the overall performance in detail with rigor and detail, and the reliability of control systems.

Now I may be misinterpreting this, because the letter is what was the terminology of the Lewis Committee used on WASH 1400?

MR. EBERSOLE: Well, except for the standpoint of calling it an undesired trip --

MR. KERR: What would you suggest?

MR. EBERSOLE: I would say they are referring from time to time to reliability systems, we refer to the range of influence that these systems have on safety problems.

MR. KERR: Okay. That's a good suggestion. Make a note of that, Dick, and I'll see how -- because the reliability may be too narrow.

Other suggestions?

MR. KNIEL: Dr. Kerr, you refer in your letter to the August 12th letter, which is the one that the Committee provided in response to unresolved safety issues, and also there is a discussion on page 2, lines 43 and 45, about the ACRS wants a broad study which reevaluates the systematic way.

I think the letter should show that both the Staff and the Commission have reacted to that August 12th letter, and the reaction to that is that designation of unresolved safety issue, and that designation will initiate such a --

MR. KERR: I think you are right, and I think that is implicit in the letter, but it needs to be made explicit. You have a good point.

Do you have that, Dick?

Other comments?

Okay, then, let me go to perhaps some additional questions that I have, at least, and that may suggest some to you.

The first question I wanted to raise is, can somebody from the Staff give me some background on how it is that one decides which systems are safety systems and which systems are controlled, or which systems are not safety systems?

MR. ROSA: Safety systems are those designated as being required to prevent or mitigate accidents. This includes safety injection systems, safe shutdown systems, also containment isolation, and all of their directly-supporting systems.

MR. KERR: I understand the designation, but in terms of a particular system, how do you decide that it fits in that category?

For example, it is certainly conceivable to me that a control system might cause an accident if it were left free to range. Now how does one decide that a control system doesn't cause or mitigate accidents, because control systems can mitigate the effects of accidents?

Indeed, that statement was made earlier, but you don't take any credit for it.

MR. ROSA: We looked at the accident analyses and the analyses associated with anticipated transients, and all systems that are taken credit for to mitigate these events are considered safety systems.

MR. KERR: You have introduced a new word into the discussion, and that is the word "taken credit for." Your earlier comment was that any system that could mitigate the effect of an accident was considered a safety system. Now you have said any accident or any system for which credit is taken, and whether you take credit or not depends on whether it is a safety system. So you have sort of a circle logic here which says that if you take credit for it, it's a safety system; and if it is not a safety system, you don't take credit for it.

MR. ROSSI: I think what is done is that you look at the equipment and at the instrumentation that is required to function in order to stay within the specified limits for either the anticipated operational occurrence or the particular accident that you are looking at. And if that equipment is required to stay within the limits for that accident or anticipated operation, then it's a safety system.

MR. KERR: Required by whom or what?

MR. ROSSI: You do the analyses and show what is required in order to stay within the limits for the particular thing you are after.

MR. KERR: But a requirement can be a very arbitrary thing. You can just pick out systems and say, "I require these to function and I don't require these to function."

MR. ROSSI: Let's say I pick a certain set of systems and I say these are going to be my safety systems. So now I draw a box around those systems and say these are the safety systems.

I then go and do a set of accident analyses which cover both anticipated operational occurrences and the postulated limiting events, and I do these analyses, and I assume that only the safety systems work, and I assume that the control systems do not work to mitigate the consequences.

MR. KERR: The choice is arbitrary. You pick out some systems and you say, "We are going to call these safety systems," and other systems, you say, "We aren't going to call these safety systems."

MR. ROSSI: Then you go test them, though. You do these analyses to make sure you have picked the right ones.

MR. KERR: Right or wrong, it seems to me, doesn't enter here. The choice is one that you make.

For example, is there any reason why you couldn't say a control system could mitigate an accident?

MR. ROSSI: Yeah, you could do it, but then once you say that mitigates the accident and it is required for a particular accident, then you have to come back and design the control system to --

MR. KERR: I agree, you would. It would then become a safety system, but the choice, it seems to me, is somewhat arbitrary.

MR. ROSSI: But I would claim there is an iterative procedure that you make a choice of what you think are the right safety systems.

You then go into analyses to test whether that is the right choice, and then if you find --

MR. KERR: How do you determine whether it was the right choice or not? That is the root of my question.

MR. ROSSI: You determine that by going through the analyses and only using the operation of those systems that you call safety systems to mitigate the consequence of each accident that you analyze, and you show that you can --

MR. KERR: But you see, by definition you have said at other points that safety systems have to be designed to mitigate the accidents, so you have defined them as capable of mitigating the accidents to begin with. I mean ECCS, for example, the criterion -- what is it, 35? It says ECCS must be a system that will in effect take care of LOCAs.

Now, by definition, that's what it does.

MR. ROSSI: That's right. And then you have to demonstrate that it does it. And if you find out in your analyses that --

MR. KERR: Well, you never really demonstrate. You demonstrate that it does with some probability. But, of course, that's left out of --

MR. ROSSI: For the certain set of accidents.

MR. KERR: And you don't necessarily demonstrate, for example, that other added systems might not do it better or improve things.

I'm not trying to be critical.

MR. ROSSI: That is very true. You don't demonstrate that. Right.

MR. KERR: It seems to me, as I think about it, that to a considerable extent the designation of the system as safety or nonsafety is somewhat arbitrary. Arbitrary to me doesn't mean immoral or bad. It just means arbitrary.

MR. ROSSI: It's arbitrary with a test that it's correct, I think.

MR. KERR: Yeah, but the test always has to work, because the safety system is imperfect unless it does the job it is designed for.

MR. ROSSI: That's right. So if it doesn't work, then you come back and include more things in it, or you change the capability or whatever. And then I think that what you start out with is ideally you want to find the simplest ways to protect the plant that you can find. So what you want to do is to find a few simple things that you can do and make sure that the plant is protected, and then you concentrate your effort on making sure that you do those few simple things well. That's ideal, I think.

MR. KERR: I would not personally claim that the systems used to protect plants are simple.

MR. ROSSI: No, I wouldn't, either, but I think you would try to find the simplest ways to do it.

MR. KERR: What is it, Okum's razor, that physicists refer to, that says given two explanations, the simplest is the best? And that may be true in control systems as well, I don't know, or safety systems. But it seems to me, again, it is somewhat arbitrary.

Mr. Lipinski?

MR. LIPINSKI: The statement was made earlier that you have systems and designate them. I would like to say that process actually takes place in the reverse direction. Chapter 15 requires certain accidents to be analyzed, and when you do the analyses -- say you get an overpressure transient, you then say, well, I am seeing a pressure rise. How do I keep the pressure within the prescribed bounds? You then define a system that maintains the pressure within limits, and if it is required to keep that vessel from rupturing, it gets a designation of a safety system. You have to analyze --

MR. KERR: But, Walt, in the process, you ignore any contribution from the control system.

MR. LIPINSKI: That's right. On these accident cases, you are looking for major deviations, rod withdrawal, the power is going up.

MR. KERR: I am simply saying I could think of a world in which one could call the control system safety-grade, and one could then look at its contributions to mitigating accidents, and I don't see anything that would violate the present philosophy other than the Staff happens historically not to have designated control systems as safety grade.

MR. LIPINSKI: There is now an economic consideration. They can be safety grade, but then you are going to follow the single failure criteria, because that's what follows.

MR. KERR: I'm talking about how one chooses between safety systems and control systems as safety-grade or not, and I don't see a clear guideline other than a choice. I mean one makes a choice and goes in there.

MR. LIPINSKI: In doing [illegible] accident analyses, you require certain systems, double pipe break for the safety injection systems. You're told to analyze that event. Prevent core temperatures and --

MR. KERR: Of course you do now, but suppose we started this process out and we decided that control systems ought to be safety grade, too. Then we might well look at the contributions that control systems made to mitigating the accident.

MR. LIPINSKI: If you do an accident analysis and say it's required to mitigate the accident, and you are calling it a control system, then it ends up being a safety system with the same label.

MR. KERR: That's my point. Had we started out making control systems safety grade, we might have them mitigating accidents.

MR. LIPINSKI: Okay. But there is another class of systems that are used to operate the plant around nominal operating points, and those are your control systems. They are not required for bounding accidents.

MR. KERR: I don't know what nominal operating points means. Let's take the ATWS issue, for example. We have discovered, in exploring the ATWS issue, that the so-called safety systems, scram system, was being used as part of normal operation, because there were certain anticipated transients, and to me, that means something you expect to be able to have to control that required scram to occur. Otherwise, the plant got in trouble.

Now I would say in this situation, what we used to talk about as a safety system is really part of the control system, because it is being used to control the plant around nominal parameters.

MR. LIPINSKI: There was earlier reactors where you had two separate sets of rods, and they were designated control rods and safety rods. As the cores got bigger, there was not enough room for separate classification of rods, so the rod systems had dual functions. They now control as well as the safety function for fast reinsertion of negative reactivity, and it's only that part of the system that gets classified as safety grade.

The ability to position these rods to maintain power is not safety. That's a control function.

MR. KERR: My point is, it seems to me this designation is pretty arbitrary.

MR. LIPINSKI: I see a defined boundary.

MR. KERR: You and Epler helped develop this, and you understand it and agree with it, and I think it's a good -- when I say this system is arbitrary, I don't mean it's bad. I just mean that could have taken --

MR. EPLER: Please. There are three. You're trying to make it into two. There is a system for control that is not required to be redundant, not required to be tested, not required to be anything except just to perform.

Now we have many of those systems. You can call them control or nonsafety.

Now we have another system that's very important. It is required to be redundant, it's required to be tested, and tested in such a way as not to impair its performance during the conduct of a test, not to be used for any other purpose, and a lot of good things. Those are called protections.

Now we have a third system which is in between. We call it safety-grade. It's neither control nor does it adhere to the principles that apply to protection. It's simply general purpose plant systems that are beefed up to make them work a little better.

Now it isn't arbitrary. This is the way the plants have grown, so let's not talk about safety and control alone. Let's talk about three kinds of systems.

MR. KERR: That doesn't make them any less arbitrary, but I'm willing to talk about three if you want to increase the arbitrariness.

MR. EPLER: That's the way life is.

MR. KERR: I guess what I'm trying to look for is some rationale that says control system -- I would assume, for example, that one might look at the ability of a system to cause accidents, and if one looks at the contribution to transients, I am not sure but what the control systems are likely to cause more transients than, say, engineered safety features. And on that basis, I could argue that maybe control systems ought to be reliable.

MR. EBERSOLE: What do you call engineered safety features, Bill?

MR. KERR: Well, in a general way -- I'm not going to try to take into account everything -- but I would say the control of the ECCS system is an engineered safety feature. It's designed to withstand reliability greater than control systems are. It seems to me I could make an argument that would say control systems in the long run are likely to contribute more risks than malfunctions of the ECCS systems. I'm not sure I could prove that, but I'll bet I could make a pretty good argument, and therefore control systems ought to have higher reliability than they now have, or at least there ought to be some reliability standards.

You could have -- and, indeed, I think the Canadians do, they did several years ago -- some standards of reliability for what we call control systems and have different standards of reliability for safety systems. That seems to me a logical approach. It's not the only one.

MR. EBERSOLE: Are we talking in a compartmentalized or general context?

MR. KERR: I don't know the answer to that until I know what you mean.

MR. EBERSOLE: Do you call the service water system a safety system?

MR. KERR: It depends on what the service water system is doing.

MR. EBERSOLE: It moves heat out of the plant, and it's the only way to move it out.

MR. KERR: Is moving heat out of the plant necessary in a given situation?

MR. EBERSOLE: Yes.

MR. KERR: Then I would want to know what one meant by safety system, because these definitions are pretty stylized. Gor example, the control system of a nuclear power plant is designed to control the system in such a way that it moves heat out of the plant.

MR. EBERSOLE: The control system is never going to move heat out of the plant.

MR. KERR: It controls the plant so that heat is moved out of the plant. That's the objective of it.

MR. EBERSOLE: But the safety system embodies, as a matter of fact, the final action --

MR. KERR: But why does one wait until one gets to the final action? It seems to me a plant is safer if it never gets into trouble than if you wait until it gets into trouble and have an absolutely safe system to get it out of trouble.

MR. EBERSOLE: That's what it does. It keeps it out of trouble.

MR. KERR: And, therefore, it seems to me that on the logic that the control system, above all, ought to be reliable. It ought to be the most reliable thing in the plant.

MR. EPLER: Mr. Chairman, we do indeed have a control system that has been made reliable, and we have a patent on it. It consists of three channels, each with its own instrumentation, three operating in parallel. They are velocity servos, so if velocity is added, one motor will turn in this direction, one turn in that direction, and one sit in the middle like Lucky Pierre, and we'd look at it and say it can't fail, there is no way it can fail. But we know it will. After years of operation, indeed, it did fail. It failed like this:

Since it was infallible, and there were three channels, it is possible to do maintenance on line, so the battery -- there is a battery for each of these three servos -- the battery was being maintained. When the maintenance was finished, it was desired to connect and reconnect the third channel which is being maintained, and a technician was dispatched to go and be sure that the battery was not reapplied without instrumentation information. Otherwise, the thing would blow its brains and go crazy. We wanted it go on smoothly and under control.

So the technician went to disconnect No. 3. He went to the back of the board and counted off one, two, three, and disconnected it. That was the wrong one. He should have gone to the foot of the board and counted off one, two, three.

So now we've got an excursion. That's the way it fails. Now I don't think you go very far by making control systems infallible. You can wear yourself out, but you don't really get very far down the road. We've been down that road.

MR. KERR: The word I used was "reliable," not infallible.

MR. EPLER: It has to perform, and it has to perform reliably. There is a limit to what we can do.

MR. KERR: Ep, I am not implying -- in fact, to me, there would be some logic in counting and calling both the control system and what is now called the protection system a control system. It seems to me that it doesn't quite make sense to talk about controlling a plant only when it's in normal operation. I think you want to control it all the time, as best you can. And therefore, I don't see really any great reason for distinguishing, at least intellectually, between the control and safety systems.

MR. EPLER: Here is the classical system, if I may. The control system is a system whose failure can be tolerated. A protection system is an independent system whose failure we cannot tolerate.

MR. KERR: But safety systems will and do fail, so if you do that, that definition to me doesn't make any sense.

MR. EPLER: Like the man said, nobody is perfect.

MR. KERR: By the way, I have a recommendation. I really think these horror stories you have, which are quite illustrative, ought to be recorded and put on cards and numbered. You know, it would be 1 through 20, and then all you would have to do is refer to No. 7.

(Laughter.)

Because they really are worth --

(Laughter.)

MR. LIPINSKI: Prof. Kerr, I would like to pursue the discussion. Let's talk about flex control as an example. If you are at 100 percent power, and you've got a load following the system, you would like to control the reactor power, let's say the turbine cuts back to 95 percent, automatically you would like to reduce nuclear power to 95 percent. I have a control system that performs that function for me, and depending on how important it is to me, I design it to a certain reliability. If it fails, it may fail stationary and the turbine cuts back, my nuclear power does not, so I've got a heat imbalance. Or the thing could fail in the direction to cause a rod withdrawal, and I have a runaway, because of the control system failure. But important as a supervisory system, that detects the fact that nuclear power is above some prescribed limit, and that is where the plant protection comes in, on a limit on the nuclear power protection.

Now we have a question of reliability, and this is where ATWS comes in, because that nuclear channel failure -- we are looking for a probability of failure on the order of 10^{-6}, whereas that control system failure right now is based on economic importance to the designer to as what he wants to prescribe for its reliability. But now we are getting into these accident cases to see whether the control system is running away in different combinations and can cause accidents to progress along some different path, other than looking at a single rod runaway, because the control rod has failed.

But there is a big difference between a control system for nominal failures versus the runaway conditions or the safety systems that come into play.

The same thing applies to water level control in the steam generators.

MR. KERR: What you are telling me, Walt, is if I lumped all this and can call it a control system, there would be certain functions for which you would want higher reliability than others. I agree. I think that's completely logical. You would not necessarily require exactly the same reliability of all components and subcomponents, but it seems to me to be somewhat arbitrary, and I must say personally strange to have no reliability requirements on a control system, and have the rather extensive requirements we now have on safety systems, and I don't really understand why we do.

MR. LIPINSKI: I perfectly agree with you on that issue, but there is a difference and I think we wouldn't want to impose the same reliability requirements as we do --

MR. KERR: I don't know what we should be imposing on the control system. Maybe indeed existing control systems meet what one would want if one looked at it. I have an idea that this is a fairly important economic issue, and I would assume that people who build these things want them to be fairly reliable, and they may indeed be. I don't know.

MR. LIPINSKI: If they are not, they are going to challenge the protection system. They are going to have unwanted shutdowns.

MR. EPLER: There is something elementary that is being over looked here. A control system must operate in two directions: up and down. That's its mission. It has to be optimized to do this. It can make a condition safer or less safe.

A protection system can operate in only one direction: a safe direction.

Now you have to keep within the limits of optimization. That's pretty elementary.

Now you can make a system that won't fail, but it won't work very well.

MR. KERR: Ep, I have never advocated making either a control or safety system that can't fail, because I think it is impossible, and in Heaven maybe one can do this, but I can't do that.

MR. EPLER: You can make it less prone to failure.

MR. KERR: All I'm saying is I don't understand why we have very high reliability requirements on safety systems, and no reliability requirements on control systems. And maybe a very good reason is I'm unaware of it.

MR. EPLER: The answer to one is by definition you can tolerate the failure of one, and the other one you don't wish to tolerate.

MR. KERR: I would say that judgment is somewhat arbitrary, and we have had control system failures which I would not want to tolerate if I had a choice, because I think they got me in situations that I would not want to be in.

MR. LIPINSKI: Let me add to that, to just arbitrarily scram the reactor every time is not a safe condition, because of the thermal conditions, such as now if I have a feedwater controller that's giving me frequent shutdowns and thermal shocks reflected into the primary system, that is not a good condition. And if this were a condition occurring frequently, somebody would take an immediate look at that problem.

And the reverse part of that is the failure rate, because if the system is unreliable, that means it's failing frequently, and the specification on a control system in terms of unreliability says how frequently can you expect that system to fail, and if it's failing too frequently, causing the plant to go through changes that you would like to avoid, then you require a specification on the systems to prevent that.

MR. KERR: Well, I don't find anything with which I disagree on that. It seems to me maybe that is implicit in what is actually being done in the review process now. But it is not explicit because what I hear is we really want to design so that that safety system can handle any excursions, but we are not too concerned about how often those excursions occur.

MR. MATHIS: I think we are.

MR. KERR: I'm not talking about what you are, I'm talking about what I heard this morning. I didn't hear any things about problems with the frequency of challenge of the safety system.

Now I have heard that in other publications of the Staff. In fact, justification for changes in set points and other things post-TMI have been made on the basis that we do not want to challenge the safety system.

Now it seems to me if one doesn't want to challenge the safety system, this implies some sort of reliability requirement on whatever it is that challenges the safety system.

MR. EPLER: There is one point that is being overlooked, and I think it is extremely important. A protection system having a failure probability of 10^{-6} has no economic importance at all. You couldn't care less. It may cost you a penny a year.

However, a control system that fails regularly is going to affect your pocketbook. We have an enormous incentive, economic incentive, to keep these things on line, and that's just great, I love it.

Now if you have got the economic incentive working for you, don't knock it, but you cannot have the economic system working for you on protection system, because if we believe our reliability failures, they are far beyond that threshold.

MR. KERR: Well, Ep, when one looks at what even TMI-2 is costing the industry, it certainly seems to me there is an economic incentive for a very reliable safety system, and I just cannot buy the argument that says people who operate plants aren't interested in safety. Maybe a few dogs aren't, but most of the people have got to be interested in safety, or they are not going to be in the business very long.

MR. EPLER: All I said was if it's 10^{-6} like we are led to believe, then they are not a matter of concern. Obviously we have systems that are not 10^{-6} and that's different ball park.

MR. EBERSOLE: I guess you are developing this topic we are coming up on about developing the importance of the forthcoming thing about identifying the meaning of systems important to safety, or safety-related, or safety-grade, or safety systems.

Could we use as a model perhaps the AC power system? The diesel generators are safety systems in my view. And one certainly does not want to challenge these things very often, because they are not so reliable.

Therefore, at the front end of these diesel power systems, we have the preferred power systems, and we call them important to safety, and we go out in the switchyard and require two lines at least on certain characteristics about switching the circuits out there. There's a gradient from the switchyard to the internal distribution system finally down to the diesels.

where the reliability is certainly not getting any better, because we well know the reliability of the diesels is worse than that of the offsite systems. But the terminal function of the diesels is to prevent a disaster, and we have stringent requirements on those, although we know that all of our efforts to do so are not going to make them very good. They are safety-grade because they, in a terminal sense, prevent a disaster from occurring when we lose in fact a better system.

T.4

MR. KERR: You are raising an important issue, and you remind me that at the present time we really don't have any reliability requirements on any of this stuff. We do have some nominal requirements on the ability of diesels to start and run, but no requirements on the reliability of the power supply.

MR. EBERSOLE: We could have parallel Goldbergs and call it a safety system.

MR. KERR: Well, my point is -- well, I don't know what my point is, except I think that one needs to talk in some sense about total system performance, rather than taking out little pieces which I have an idea is what we are now doing.

MR. LIPINSKI: To summarize, you are only pointing out the inadequancy of the single failure criterion, because as a minimum you have two diesels, yet their combination together in terms of their overall function is pretty low. In terms of their being required to remove residual heat, if we do not have offsite power. And the question is, what should their overall system reliability be.

MR. EBERSOLE: Which involves the reliability of what we would call the control context or the systems important to safety, but not the safety systems. It's a composite problem. It's a composite problem. One is dedicated to not having a high challenge rate to the final line.

MR. KERR: Are there other questions or comments?

Let me ask the Staff, if you were starting from scratch and did not have all this tradition for which Epler or Ebersole are responsible, probably partly --

(Laughter.)

-- of controlling safety systems, do you think you would do it this way the second time over? That is, would you make this very sharp distinction between reliability requirements for safety systems and in effect very little reliability requirement for nonsafety systems?

MR. ROSA: Speaking for myself, I do not believe there is another approach that can be followed that would get us where we are now, frankly.

MR. KERR: I think that is a statesmanlike answer.

(Laughter.)

Because I don't think there is another approach, either, that would get us where we are now.

(Laughter.)

MR. ROSA: Where we are now in terms of safety, in terms of nuclear power availability, and so forth.

MR. KERR: I am not criticizing where we are now, but it is possible in hindsight, one generally thinks one can do a better job, and I just wondered if, with hindsight, and you had it to do over again, you would make this sharp line of demarcation between safety and nonsafety systems. I know Epler would, so -- I mean would not.

MR. EBERSOLE: Bill, one thing --

MR. KERR: Wait a minute. I'm not trying to force you to say something you don't want to say.

MR. ROSA: The only basis for another approach which is making the control system a safety system would have --

MR. KERR: Please, lest there be a misunderstanding, I am not saying control systems ought to be safety-grade. I don't know. I am suggesting that maybe there ought to be some reliability specification, but even then I am not sure.

MR. ROSA: If we had started out with a set of reliability requirements in terms of numbers, fine. We could, I think -- I think design a system, a control system as well as a safety system, perhaps in a different manner. But there was no way to arrive at this point of having numerical reliability criteria and until you get a number of operating plants and a date base established, that won't happen.

MR. KERR: I guess what I should have said is if you were starting now with a date base you have, and without the tradition and all the rules and regulations, would you still do it this way?

MR. ROSA: If I were starting now, knowing everything we know now, I would say this: I would say that the frequency of challenge of this safety system that results from control system failures is a growing concern, and that therefore we would take a closer look at the design of the control system, and also the operating experience of each new design as it came on line, and we would also recognize that every challenge of the safety system due to control systems is an economic penalty on the utility, and that that primarily should be relied upon to produce a reliable system and improvements as necessary, as operating experience dictates.

Now I emphasize that this is my opinion.

MR. KERR: Other comments?

MR. EBERSOLE: Well, the safety systems, as you well know, have to be environmentally qualified for a host of things that control systems don't have to be qualified for.

For instance, you don't expect earthquakes, storms, protection from fires, et cetera, wherein from a commercial viewpoint you would be willing to take a failure, and you are not entitled to take that failure --

MR. KERR: No, Jesse, if I suggested that control systems ought to have reliability requirements, I would be surprised if it turned out you would want them to be as reliable. But that doesn't mean they should have no requirements at all. My mind isn't made up on this score at all. I am just really trying to do a sensitivity analysis, if you will.

MR. EBERSOLE: I don't have any difficulties seeing safety systems redlined as differentiated from control systems. That applies to service water, hydraulics, mechanical systems, not just electrical apparatus.

MR. KERR: Mr. Rosa?

MR. ROSA: Mr. Chairman, I think as a result of the work that is going to be done on this task, generic -- well, the issues, the generic issues task that we talked about before, an analysis of the LERs related to -- or involving control system malfunctions which will distinguish between control system malfunctions due to human error as opposed to control system malfunctions due to actual equipment failures or power supply failures will provide the insight that is necessary to develop criteria that can be applied. But in the absence of an analysis of this sort, I don't think we can proceed to do anything right now, except what we are doing.

MR. LIPINSKI: Steam generator overfill is another good example. If every time we tripped the turbine, we were to fill that steam generator with the probability of bringing the steam line down around our neck, we would quickly change our philosophy on the design of that level control system.

And right now the analysis may come out with further analysis in making it safety grade.

MR. EBERSOLE: I think what will happen is it might increase the reliability because of the implications of commercial damage and shutdown.

On the other hand, I think what will come out of it is it will now be recognized that that particular control system must be -- must have an adequate safety system override to control its malfunctions. Consider the rate of the function. But it may be that that system may not get any better, but it will be in place. Another system that will cope with its malfunctions.

MR. KERR: Gentlemen, I need your advice.

MR. ROSA: May I have one more comment, sir?

MR. KERR: After I get the committee's advice. As I listened to this discussion, which I find very illuminating, it's my guess that after a break, about an additional hour of discussion, we will have exhausted most of the new ideas we are about to come up with at this meeting.

My question to you is, shall we continue this for about another hour and then call it a day? Or do you want to break for lunch?

MR. MATHIS: Continue.

MR. KERR: And is there any disagreement with my judgment as to the value of continuing this discussion beyond an hour? I would guess that that will have exhausted most of our fresh and new ideas.

Let me suggest, then, that we take a 10-minute break and continue -- plan on continuing for about an hour after that. May I? And, Faust, I will get right back to you.

Does the Staff have any objection to this procedure?

MR. ROSA: None at all that I know of.

MR. KERR: Okay. Thank you.

(Recess.)

end AR Beach fls.

MR. KERR: Mr. Rosa, you had some comments which I interrupted. Why don't you continue.

MR. ROSA: Okay. They'll be very brief.

Going back to what I had said previously about safety systems, or those that are taken credit for in the safety analysis, I just simply want to state that the Staff uses that term "take credit for" in safety analysis rather frequently. What we mean is exactly the process that Dr. Lipinski described, when we use that term.

The other comment I had to make is simply this: When we're talking about making control systems "safety grade," what we're really saying is: We ought to have some redundancy built into the system such that it's not subject to single failure. I think we can eliminate the need for environmental protection beyond capability for operation in a normal environment, or for seismic capabilities, because we are concerned with just challenges to the protection system of control system failures in the -- during normal plant operation.

That means that to apply the single-failure criterion to an already very complex system is going to add additional complexity. I am reminded of what some people describe as a natural law in the protection area that "simple is safe." It seems to me that if we go overboard towards providing single-failure requirements to control systems, we may be adding less reliability than we think. In fact, we may be degrading reliability. That's the only thought I had.

MR. KERR: Okay, let me comment on those thoughts in reverse order.

I have heard the same expression, that "simple is safe," the implication being that it is desirable to design simple systems. I'm not quite sure why it is that simplicity appeals to so many people so much. But as I look at the world around me, I find that one of the more complicated living organisms is the human being.

I would certainly hate to eliminate all of them just because they're not "simple" --

(Laughter.)

MR. EPLER: They will be.

MR. KERR: They do have characteristics that make you want to eliminate them, on occasion, but I think sometimes complicated systems have virtue. So I just wouldn't want to completely eliminate that possibility.

The second had to do with your earlier comment, which I think was well taken, about the need to study the question in some detail before deciding what the correct approach would be.

You mentioned that you were going to use the LERs for this purpose. I am not the first to indicate that LERs are somewhat deficient in being able to provide information.

I think Mr. Basdekas pointed out this morning that not every failure incident -- or in fact I'm not even sure the majority of failures of control systems are covered in LERs. It would seem to me, therefore, that one would want to supplement the LERs with some other source of information.

One possible source, it seems to me, would be a failure modes and effects analysis -- although, for the life of me, I've never been sure I understood what one meant by that, but I understand there is such a thing; and indeed, the Staff required B&W to do one, and even asked Oak Ridge to comment on it.

I guess, if I can follow that comment with a question: Why did the Staff require this of B&W, but not of anybody else? Can somebody --

MR. ROSSI: Well, I think there was a feeling from some incidents that had occurred on B&W plants, and also from looking at the B&W design, that the integrated control system on B&W may have tied the control of many functions together more closely than had been done on other vendor plants. That was, I think, the reason that that one particular vendor was asked to do this.

MR. KERR: I guess I am not sure what is meant by "tying the events together closely."

MR. ROSSI: There were control functions that affected many variables kind of simultaneously in the integrated control -- just the very fact that it was an integrated control system where the philosophy was that you try to vary several things at the same time for power changes and during other plant transients with the control --

MR. KERR: I could interpret what you're saying to mean that because they had a control system that controlled, then you were concerned about the failure thereof; whereas other plants have control systems that don't really control very much --

MR. ROSSI: Well, no. I think the other plants have control systems that control, but they are a little more separated in the way they do the functions --

MR. EPLER: More eggs in one basket.

MR. ROSSI: More eggs in one basket on the B&W, perhaps, than on the others.

MR. EBERSOLE: Well, isn't it true that that system is a tight system because of the relatively low inventory of water on the secondary side?

MR. ROSSI: Well, that's right. I think that the --

MR. EBERSOLE: In order to avoid excessive scrams and turbine trips --

MR. ROSSI: They required this; right. They had to have a more tightly coupled system.

MR. EBERSOLE: The end result of your imposition on them now is they're going to scram more often, which may or may not improve the safety picture.

MR. ROSSI: From -- you mean from the standpoint of changing setpoints that --

MR. EBERSOLE: I mean, you're going to make them scram more often.

MR. ROSSI: Through what? Through the changes --

MR. EBERSOLE: Decoupling some of the things that were previously coupled.

MR. ROSSI: Well, that could happen. I don't know that we've asked them to decouple anything that was --

MR. EBERSOLE: Well, you've got turbine trips now --

MR. ROSSI: Yes. The kind of things we're looking at is power supply --

MR. KERR: Well, if you found out you were increasing the number of scrams in normal operation, would that be a concern?

MR. ROSSI: I think that would be a concern.

MR. KERR: Have you checked to see?

MR. ROSSI: That would definitely be a concern.

MR. EBERSOLE: Isn't that rather obvious that that is what is going to happen?

MR. ROSSI: Well, not necessarily, because if you try to divide things up maybe a little better on power supplies, it's not clear that you would end up with more scrams.

MR. EBERSOLE: So that's not clear, yet?

MR. KERR: Has anybody looked to see if you're getting more scrams?

MR. ROSSI: I don't think a systematic look has been taken at that; no.

MR. LIPINSKI: Well, they were directed to provide turbine trip; whereas, the -- They were directed to provide a turbine trip; whereas, the original design of that integrated protection system was to ride out the turbine trip.

MR. ROSSI: That's right.

MR. LIPINSKI: That trip has now been added, so that every time the turbine trips, the reactor scrams. So their frequency has to go up.

MR. ROSSI: So that will make it up; yes, certainly.

MR. LIPINSKI: Because some of those events they were able to ride out by previous design; but now, by mandate, they must trip.

MR. KERR: Now, let's see. It seems to me also that I read a letter recently in which Westinghouse was being required to install an anticipatory trip because otherwise there may be too many challenges to the safety system.

So there is a Staff position which, in a sense, says we want to modify the control system, or at least the nonsafety part of the system -- or maybe that now becomes part of the safety system to avoid challenging the safety system.

Is that Staff philosophy, now?

MR. ROSA: I'm not familiar with the anticipatory trip you referred to. Does anyone on the Staff here --

MR. KERR: I could look up the letter. I should have written the reference down, I guess, but it was one of these letters that come across my desk that I happened to read.

MR. ROSA: I recall an anticipatory trip item in the lessons learned.

MR. KERR: Well, this was a letter to Westinghouse. Apparently there had been some disagreement, and the Staff was saying: You've got to put in an anticipatory trip because we don't want -- and I quote -- "challenges to the safety system."

MR. ROSSI: I can't talk about the specific thing that you're asking, but let me bring up a kind of a philosophical point on challenging safety systems.

I think that you might put in an anticipatory trip which would trip the reactor more frequently if by putting that kind of thing in you found that you would reduce the number of challenges to overpressurizing the reactor coolant system, or reduce the number of challenges to defeating the heat removal from the reactor coolant system.

So I think you have to look at whether or not in some cases it might be better to have more reactor trips and fewer challenges where you might end up without being able to remove heat from the core.

MR. KERR: Okay, I guess I didn't make my question very clear.

In your presentation earlier, the impression I got was that the number of trips was not a matter of concern; what you tried to do was make certain that you could handle any sort of malfunction or aberation of the control system by the safety system; and that if a trip took care of it, that was it. You didn't count number of trips and say that if we get more than 10 or 100, that's a problem.

MR. ROSSI: I think in terms of the Regulations and the way we license plants, that's true. I think that there is a concern on our part --

MR. KERR: I'm sorry, but any letter that goes out from this Staff to Westinghouse telling them that they've got to put on anticipatory trips is part of the licensing process. To me, that represents evidence of a Staff philosophy. Now it may not to you, but I bet it does to Westinghouse.

MR. ROSSI: But again, I think that would only be done if, by having an additional reactor trip, you could minimize the challenge to other safety functions.

MR. KERR: I don't disagree with that; but what I am saying is: If your argument for not having any specifications on the control system is, "we really don't worry about, implicitly, how many challenges; we just design the safety system so it'll handle them," --

MR. ROSSI: Okay --

MR. KERR: And then we don't look to see how many challenges the control system is going to provide.

Here is a situation, it seems to me, in which the Staff is saying: Ah-ha! You've got too many challenges to that system; we've got to prevent that.

Therefore, one could interpret that as being somewhat inconsistent. I don't.

MR. ROSSI: I guess there would be somewhat of an inconsistency, perhaps --

MR. EBERSOLE: Bill, I can't separate. The number of challenges is an integral part of the safety problem.

MR. KERR: Jess, I don't disagree with you. I'm saying that I didn't hear anything about number of challenges in the presentation this morning. What I heard -- maybe I misinterpreted it -- was that if we design the safety system so it will take care of a challenge, the number of challenges is not a problem.

MR. EBERSOLE: But it is, because of the reliability problem of safety systems.

MR. ROSSI: Well, the number of challenges have not been the subject of reviews. I think that's fair. I think that there is a concern, and there may be some inconsistency in what we have done. But I think that in the licensing process in general that the number of challenges and the number of reactor trips has not been a concern; but the concern has really been that when you get them, the systems will keep you out of trouble.

MR. EBERSOLE: Pardon me. You can't say that in a general context, because when you go out in the switchyard and look at the distribution systems and the preferred power supplies, and the number of incoming lines, obviously you were working toward reducing the number of challenges to the diesel power system, for a good reason.

MR. ROSSI: Okay.

MR. EBERSOLE: Now you may not have done it to the scram system, but that doesn't mean you shouldn't.

MR. ROSSI: Okay.

MR. EBERSOLE: I think it's just like the persistency about looking at the number of challenges. Obviously you felt that you don't want to start the diesels under duress any more often than you have to. So you've put a lot of impositions and gradations in safety from the switchyard on in.

MR. ROSA: I agree with you. And as I said before, I believe the Task plan will include taking a look -- a rigorous look -- at the experience of challenges to the safety system.

MR. KERR: Let me explore another issue a little, if I may. There is currently a great deal of interest on human-factors' engineering that is being manifested by rather detailed analyses and some changes in control room design.

Now is one restricting that to the safety systems and their indicating instruments? Or does that interest extend beyond safety systems to control systems, as well?

MR. ROSA: I believe it extends to the entire system -- safety, as well as control.

MR. KERR: Well, again, it just seems to me to be a little inconsistent with the philosophy that says that if we design the safety systems to handle incidents, we don't have to worry about the performance of the control system. Here, it seems to me, is a situation in which one is saying that interaction between people and control systems has been less than satisfactory in the past, and we're going to try to do something about it.

MR. ROSA: Well, we don't expect that the automatic actuation of safety systems will be sufficient, unto itself, to mitigate completely any accident or transient. But some human actions have to take place sometime --

MR. KERR: Here is a situation, it seems to me, without setting a quantitative goal, that something is being done which will enhance the reliability of the control system, assuming that the human being is a part of that.

MR. ROSA: That's true.

MR. KERR: Okay.

MR. EBERSOLE: But something is also --

MR. KERR: And in fact, rather detailed reviews of this part of the control system are taking place.

MR. ROSA: Yes, that's correct.

MR. KERR: Okay.

MR. EBERSOLE: Bill, may I ask a question? You are going to get into this topic here, as you appear to be getting into it, of the matter of the gradation of QA and QC, as you go from systems which are called "safety related," or "important to safety," and finally proceed to the ultimate which is the safety systems? You appear to be touching on this topic which is really sort of a future topic. Did you intend to carry it much farther? I'm talking about the gradation of safety requirements.

MR. KERR: Well, you'll remember in Oklahoma where, in Kansas City, they've gone about as 'fer as they can go'?

(Laughter.)

MR. KERR: I want to go just as 'fer as we can go within six months, as long as it bears on this topic. And as I view the topic, it does involve some retrospective look, if you like, on reliability and performance requirements of those things that affect the safety of a nuclear power plant. And I am personally convinced that probably control systems do have some influence on safety.

MR. EBERSOLE: Well, control systems are analogous to, for instance, preferred power versus a dedicated power system.

MR. KERR: I would say, almost any system that has something to do with plant operation eventually has some influence on safety, and one needs to try to make some gradation among those systems. I don't think one would come out with a requirement that said all systems should have the same reliability requirement.

MR. EBERSOLE: Right. Well, let me ask Faust. Do you have in place, or could you produce now, your philosophy that expresses your gradation in QA and QC as you approach the ultimate system like, for instance, the diesel plan or the scram system, from some distant place like the switchyard, or some challenge point off in the distance? Do you have in place now an unstated activity that defines increasing quality control and QA -- for instance, resistance to seismic events, et cetera -- as you approach the final wall of protection? It's not expressed, and it's very unclear, and it gets to be a big flap.

You know, right now there is an effort and Congressional activity to make them all good, all the best, which I'm sure is not practical.

MR. KERR: Do you understand the question?

MR. ROSA: Yes, I understand the question.

We have Class IE systems, complete safety grade systems. Of course everyone understands what they are. Now we have applied, in the course of our review, what we call "equivalent requirements" with regard to, say, oh, a Class IE for nonredundant components of the nonsafety system.

A case in point is the off-site power system from the safety buses to the switchyard. That's not a Class IE system. However, we do require that this be high-quality industrial grade, and that a QA program be in place at the construction site and at operating sites following initial operation that monitors these systems.

So, yes, there are criteria in place that are applied. However, it's not formalized as --

MR. EBERSOLE: That is the problem. I think now what is happening is, because of issues of Safety Boards and other things wherein one must say why they're not all of top grade, that something has to come out to express why they don't need to be. You know, gradation needs to be expressed and the reasons for it.

MR. ROSA: Well, I guess the basic reason why we don't have a complete set of criteria in place that addresses the gradation of requirements is this: It is simply that the regulatory process is an evolving process. We couldn't start out with the system in place; it had to grow as we went along.

It is doing that now, and this effort in IEEE is the latest activity towards attaining what you would like to see.

MR. EBERSOLE: Well, in the final analysis, isn't it true that all of this is done simply to reduce the challenge frequency to the final system?

MR. ROSA: That is certainly part of it, yes.

MR. EBERSOLE: Isn't it the bulk of it?

MR. ROSA: Well, no, because it is to reduce the challenges to an ultimate safety system. Or it could be simply to make a nonsafety system more effective in mitigating accidents, for instance. The off-site power system is a case in point, to make it more reliable, if you will.

MR. EBERSOLE: You mean, in preventing --

MR. ROSA: In preventing; right.

MR. EBERSOLE: To control its range of influence?

MR. ROSA: Well, here you enhance safety by providing an off-site power system, which we call a nonsafety system, that is highly reliable, because now the overall AC power availability is increased.

MR. KERR: Let's see. Earlier you told me, I think, why you asked for a failure modes and effects analysis for B&W. You didn't tell me why you didn't require one for the other plants. Maybe I should ask that. Or maybe I should also ask: As you go into this study, is it likely that that would be useful enough that either you would do one, or require other vendors to do one, or somebody, on their control systems?

MR. ROSSI: Well, I think the "why" was that we started out with the B&W one. We are still -- you know, that has been done; it's been reviewed by Oak Ridge. We are still discussing it with the licensees. I told you why we started with it, first, and I don't think we have fully considered yet what we are going to do, if anything, with the other vendors. I don't think we've closed that, yet.

MR. KERR: Did you find the analysis useful?

MR. ROSSI: Well, let me give you my personal opinion. My personal opinion is that probably more effort was expended in it than what we got. That, I guess, would probably be my personal opinion on failure modes and effects analysis, that you probably don't get enough out of them to warrant the effort. And I think there may be better approaches.

MR. BASDEKAS: Mr. Chairman?

MR. KERR: Yes, sir.

MR. BASDEKAS: May I comment on this point?

MR. KERR: Yes, sir.

MR. BASDEKAS: The failure modes and effects analysis was requested by the Staff of B&W plants right after the TMI accident. The Lessons Learned Task Force reported -- I believe it's NUREG-585, if I'm not mistaken in the number -- that the same should be done with respect to control systems of other vendors.

I understand that later the Staff backed off from this advice, or commitment, whatever it might have been. The reasons that were given by Mr. Denton to Chairman Ahearne on December 17th, 1979, during a briefing, of which there is a record. In it, without quoting -- of course I don't remember -- but paraphrasing Mr. Denton's comments, for the reasons, was that the Staff felt that the other vendors had enough other things to do; hence, they will not ask them to perform a failure modes and effects analysis.

Now the value of failure modes and effects analysis is, I think, a lot more than is envisioned by the Staff as reflected by Mr. Rossi's comments here, if it's done properly. And I think a proper way to do it, as well as a description of failure modes and effects analysis, you may find in IEEE Standard 352-1975. That is intended for the analysis during the design stage of reactor protection systems, but the method basically can be applied to 20 systems.

As the terminology applies here, you determine the failure modes of a system, and then you determine its effects on something -- in this particular case, safety. It is as simple as that. It is straightforward, and I think it can be quite productive.

As a matter of fact, in the performance --

MR. KERR: In your view, was the B&W analysis done following that IEEE Standard?

MR. BASDEKAS: Not altogether, but certainly it was --

MR. KERR: 90 percent?

MR. BASDEKAS: Well, the format certainly is pretty much along those lines. However, I think in terms of its proper implementation of that procedure, I think the B&W report left a lot to be desired. And I think some of this had been organized by the Staff --

MR. KERR: No, I mean, would you say it was maybe 90 percent correct? Or 70 percent correct? Or what -- or 10 percent? Or what?

MR. BASDEKAS: Well, I would say you don't even get to 30, 40 percent, maybe.

MR. KERR: So in your view, it wasn't really --

MR. BASDEKAS: It was deficient.

MR. KERR: -- really wasn't a very good analysis?

MR. BASDEKAS: No. But certainly it was a step in the right direction, of which I thought the Staff should have seized the opportunity to proceed to enhance the value of that study by encouraging B&W to continue, as well as initiating the same type of studies with the other vendors. I have been making that point for a long time, and I do second Dr. Lipinski's recommendation.

MR. KERR: If you had an opportunity to review the B&W analysis, what did you learn from it that was especially significant?

MR. BASDEKAS: Well, for instance, I don't believe they have -- either because of time limitations or other pressures -- they have missed some things which were very important.

One of the things they have missed was the fact that this failure of a level controller on the steam generator side of the system can cause rather severe consequences on the primary side; and the consequences, or the effects, if you please --

MR. KERR: I guess I --

MR. BASDEKAS: -- will tell you more what is indicated is of no consequence, not even of the reactor who trips, they said.

MR. KERR: No, I didn't make my question clear. I had assumed that with a 30 to 40 percent grade that you would have perhaps learned something new from it. What you just told me was something you didn't learn from it which they missed.

Was there anything new in it that you can think of that was valuable that was uncovered by their analysis?

MR. BASDEKAS: Well, I don't specifically recall, but certainly some of the things that the Staff learned from that I'm sure have been valuable, at least if not in terms of taking specific steps, at least in getting a better insight as to the things that they ought to continue looking at. I gave you just an example of having listed the failure mode of a certain controller on the secondary side. However, having failed to properly identify the effects of it.

MR. KERR: Yes.

MR. BASDEKAS: And I think that is where the value of failure mode effects analysis comes about, because it forces one to go through in a methodical way, as described in this IEEE Standard that I mentioned, and force himself to go through and ask the "what if?" questions that otherwise he might have missed, or almost certainly would have missed --

MR. KERR: Okay.

MR. BASDEKAS: -- either by coincidence or by accident.

So I think that with respect to failure mode effects analysis, let me reiterate the point I've made in my writings there for quite some time: The fact that the recommendation you heard from Dr. Lipinski this morning ought to be, hopefully, taken seriously.

MR. KERR: I guess I would be skeptical that just anybody using IEEE Standards could do a meaningful failure modes and effects analysis. My guess is that you have to have at least 15 years of experience, and a lot of familiarity with systems.

MR. BASDEKAS: Certainly, but you need a framework on which to build, absolutely. IEEE Standards do not do the work. They do give, however, some guidance gained from experience in other industries --

MR. KERR: I interpreted your comment to mean that you thought, given that IEEE Standard in the left hand and the plant drawings on the right hand, it's fairly straightforward to do one.

MR. BASDEKAS: For someone who knows what he's doing; yes.

MR. KERR: Oh, okay. That's a good qualifier.

MR. ROSA: Mr. Chairman?

MR. KERR: Yes, sir.

MR. ROSA: One of the reasons we have confidence in plant controllers is the fact that I think it's generally recognized that designing a system of this complexity is pretty nigh impossible without some extensive failure modes and effects analyses being performed -- whether they're formally documented or not.

I expect that all of the vendors have done this type of work, asking them to repeat it --

MR. KERR: Mr. Rosa, that argument would be more convincing to me if you had just recently asked B&W to do one. Maybe there was no particularly logical reason why you should have, but you did.

MR. ROSA: Well, no, I believe --

MR. KERR: And you could have made exactly the same argument you're making to me, before you asked them to do that.

MR. ROSA: I believe we have reason -- or we had reason to request that B&W do this. I think that operating experience has demonstrated that the B&W system was -- to use a term that's hard to really define -- a little tighter than the others.

MR. KERR: Well, now, let's walk through this logic slowly. Your logic was that these systems were so complicated that anybody had to do a failure modes and effects analysis in order to design them.

You then say that the B&W system is more complicated than most -- which says to me that they have to do even more failure modes and effects analysis in order to design them.

And yet, you require them to do one. And that's the point at which I get lost, but maybe --

MR. ROSA: I didn't say it was more complicated than others. I said that its operation, as observed in operating experience at B&W plants, seemed to indicate that its responses to plant transients were a little tighter than the others, and therefore might get you into trouble more often.

MR. KERR: All right, I stand corrected.

MR. LIPINSKI: Could I offer a comment?

MR. KERR: Mr. Lipinski.

MR. LIPINSKI: I haven't seen the B&W analysis, but I'm sure there is one that is in there that says the PORV opens to control reactor pressure, and the failure is: It sticks open. The effect is: The system depressurizes.

Now having identified that effect on this analysis, somewhere somebody has to translate that effect into a course of action such that that system is in use, and it has this failure mode, and how do you then respond if this failure mode occurs?

Now I'm sure B&W must have thought about that somewhere when they had the block valve in there, but somehow systematically this did not get translated into identifying all of these effects and then giving them as instructions to the operators as to what course of action they were to take if these failure modes occurred.

MR. KERR: Mr. Epler just said earlier, "nobody is perfect."

MR. LIPINSKI: Yes; even Mr. Epler didn't analyse this triplicated system for a possible failure mode when they pulled the second one.

MR. KERR: You have a very good point; I agree.

Any other comments or questions on this issue?

(No response.)

MR. KERR: In Mr. Paul Check's memorandum of December 19th, 1979, addressed to Mr. Eisenhut through Mr. Linus -- Do you by any chance have a copy of that so that I can refer to it, rather than reading?

(Pause.)

While you're looking, it is a short paragraph. It is on page two of that memorandum, and it is the first full paragraph on the page, and he says:

"Our specific concern relates to new scenarios generated by some licensees during their reviews and described in detail in their reports. Although each new scenario was resolved by the licensee who developed it, we cannot tell whether other similar plants considered these scenarios. We recommend that the scenarios described in Appendix A be addressed by the appropriate LWR licensees within the next 60 days."

Was that recommendation acted upon?

MR. ROSA: I don't know, sir.

MR. MORRIS: No, it was not.

MR. KERR: Is it still under consideration? Or was it decided not to do anything about it? I mean, was a specific decision made not to do anything?

MR. MORRIS: It was "delayed," I believe is the correct interpretation, and as I understand it now --

MR. KERR: Delayed indefinitely? Or to some fixed time?

MR. MORRIS: No, no. This issue was considered as we looked at it at the time to be an example of a systems interaction. And as we went through the reorganization process, it was targeted as an item that would be considered among the other kinds of systems interactions, and has now been adopted, I believe -- John Stoles can take the mike now, and has taken it over as far as systems interaction.

MR. KERR: So it will be treated, but under the Systems Interaction Program?

MR. MORRIS: I'll let John speak to that.

MR. STOLES: John Stoles. Ernie Rossi mentioned earlier, correctly, that we plan to include this type of review during our Systems Interaction evaluation of Indian Point 3. We haven't had a chance to really discuss in detail the program with the power authority of the State of New York because, as you know, they just elected their supporting contractor, Abasco.

We are anxious to meet with them in the next week or so to introduce the thoughts that we want to get across in their program, which in fact does include the subject that we're talking about today. That is, safety systems and control systems; and specifically, taking a harder look at the high energy line break and its consequential failures on control systems such that they might in fact effect safety systems.

As you heard earlier, the Staff looked at what the licensees brought back after the 20-day letter. There was no hard, independent review that we know about -- and I think we deserve to look into that matter further.

MR. KERR: Excuse me. I didn't understand your last statement.

MR. STOLES: I'm saying that the Staff made an evaluation largely based on the information that was provided by the licensees, and I am not aware that there was any detailed independent evaluation by the Staff on these presentations.

MR. KERR: Okay.

MR. STOLES: And I think we deserve to look into that further as part of -- for example, on Indian Point. Essentially what we're proposing is to use Indian Point 3 as a test bed to kick off this type of review, and possibly we will gain some insights into this subject.

MR. EBERSOLE: Mr. Chairman?

MR. K RR: Yes, sir.

MR. EBERSOLE: At this point, I want to be sure to reiterate, so you hear what I say: The high energy line break is probably a less likely accident than a manifold break, which directly affects the control of the safety system performance, since those manifolds, as designed in the earlier plants, simultaneously furnish information to both the safety and control systems en mass.

MR. STOLES: We understand.

MR. EBERSOLE: And you don't have to have anything impact, you just lose the signal.

MR. STOLES: Right. That's right.

MR. KERR: Are there other comments or questions?

MR. STOLES: Dr. Kerr?

MR. KERR: Yes, sir.

MR. STOLES: I thought I would remind the subcommittee that there will be a subcommittee meeting planned for February the 3rd on the subject of definition of "safety grade," "safety related," "important to safety," as they fell out of the TMI-1 restart hearings. There is a meeting scheduled for that, and we're in the process of negotiating an agenda with that subcommittee. So the subject matter that you brought up earlier will be discussed further at that February 3rd, subcommittee meeting.

MR. KERR: Thank you. That is relevant. I appreciate your calling that to our attention.

Are there any other questions?

(No response.)

MR. KERR: I have nothing further. Let me request of members of the subcommittee and our consultants that you send me a written list of suggestions for further committee activity. Based on that and what Mr. Savio and I can put together, we will schedule further meetings of this subcommittee to pursue this subject, and I hope in greater depth.

May I thank all of you for your contributions today, and the meeting is adjourned.

(Whereupon, at 1:02 p.m., the meeting was adjourned.)

* * *

NUCLEAR REGULATORY COMMISSION

This is to certify that the attached proceedings before the

____

in the matter of: ACRS - SUBC. ON ELECTRIC POWER SYSTEMS

Date of Proceeding: January 23, 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.

M. E. Hansen

Official Reporter (Typed)

M. E. Hansen

Official Reporter (Signature)

NUCLEAR REGULATORY COMMISSION

This is to certify that the attached proceedings before the

____

in the matter of: ACRS - SUBCOMMITTEE ON ELECTRIC POWER SYSTEMS

Date of Proceeding: January 23, 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)

Ann Riley

Official Reporter (Signature)

NUCLEAR REGULATORY COMMISSION

This is to certify that the attached proceedings before the

____

in the matter of: ACRS - SUBC. ON ELECTRIC POWER SYSTEMS

Date of Proceeding: January 23, 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 W. Beach

Official Reporter (Typed)

Jane W. Beach

Official Reporter (Signature)