NUCLEAR REGULATORY COMMISSION

ORIGINAL

POOR ORIGINAL

In the Matter of: ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON ELECTRICAL SYSTEMS

TO REVIEW MATTERS RELATING TO THE
USE OF COMPUTER PROTECTION SYSTEMS

DATE: February 24, 1981 PAGES: 1-253

AT: Washington, D. C.

RECEIVED
FEB 25 1981
U.S. NUCLEAR REGULATORY COMMISSION

ALDERSON REPORTING

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

Telephone: (202) 554-2345

8102260724

T

TR04

0/1

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON ELECTRICAL SYSTEMS

TO REVIEW MATTERS RELATING TO

THE USE OF COMPUTER PROTECTION SYSTEMS

Nuclear Regulatory Commission

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

February 24, 1981

The subcommittee convened, pursuant to notice, at 9:00 a.m.

ACRS MEMBERS PRESENT:

W. KERR, Chairman
J. C. EBERSOLE
J. J. RAY

CONSULTANTS PRESENT:

S. DITTO
E. EPLER
W. LIPINSKI

DESIGNATED FEDERAL EMPLOYEE:

R. SAVIO

ALSO PRESENT:

H. ALDERMAN
F. BOYD
A. PEARSON
B. MORRIS
L. PHILLIPS
M. SRINIVASAN
E. KENNEDY
A. SPINELL
T. COGBORN
T. STARR
T. ROZEK
B. GILL
W. MOODY
E. BROWN

* * *

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 Subcommittee on Electrical Systems.

My name is William Kerr. I am subcommittee Chairman. Other subcommittee members present today are Mr. Ray and Mr. Ebersold is expected. The consultants with us are Mr. Ditto, Mr. Epler and Mr. Lipinski. We are also pleased to have with us today Mr. F. C. Boyd and Mr. R. A. Pearson from our neighbors in Canada who have consented to listen in and they are also going to carry on some discussions with us tomorrow.

The purpose of the meeting is to review matters relating to the use of computer protection systems and we are going to look particularly at a Combustion Engineering core protection calculator as embodied in a reactor currently under review for an operating license, San Onofrey.

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

Mr. Savio is the designated Federal Employee for this meeting.

The rules for participation in the meeting have been announced as part of the notice published in the Federal Register on February 12th of 1981.

A transcript of the meeting is being kept and will be available by March 12 of 1981.

We request that each speaker identify himself and use a microphone.

We have received no written comments or requests for oral statements from members of the public.

We will proceed with the meeting. We have a proposed agenda and we begin with an executive session according to that agenda. The executive session will be short and indeed I guess part of it has already occurred.

The only thing I would add is that this subcommittee in its pursuit of today's review and in further meetings will be examining the philosophy and approach used by the staff in its review of reactor protection systems and reactor control systems in an effort to provide some answers to Mr. Stewart Udall's committee.

Mr. Udall has asked us to look at the staff's review practice and philosophy and make some comments. One of our responsibilities today I think will be to further explore that philosophy.

Are there any comments or questions on the part of committee members or consultants before we begin our presentation?

Mr. Ray.

MR. RAY: Is there any intent to make the results of this discussion part of the input to the San Onofre operating license review? Is there any purpose?

MR. KERR: Mr. Bender specifically asked that some of the specific topics being looked at today be looked at by this subcommittee as part of that review, yes.

Other questions or comments?

(No response.)

MR. KERR: There being none, I will ask Mr. Kennedy, who is here from Combustion Engineering to begin the presentation.

MR. KENNEDY:

INTRODUCTORY REMARKS OF

ERNIE KENNEDY OF COMBUSION ENGINEERING

MR. KENNEDY: Thank you, Dr. Kerr, and good morning [illegible]men. My name is Ernie Kennedy. I am Manager of Project and Generic [illegible]ing at Combustion Engineering and we are happy to be here today.

As you stated, our purpose in being here today is to discuss computer based reactor protective systems. As you are no doubt aware Combustion Engineering from some time has used computer technology in some of the reactor protective functions in our protective systems. Those we have called core protection calculators.

We currently have one system operational at Arkansas Nuclear One Unit 2. The second of these systems will be going into operation in San Onofre Unit 2 which currently is before another ACRS subcommittee pending its operating license review.

We will in large part direct our presentation and our comments to those two plants since they are of particular interest to you.

We have an agenda which I would like to go over very briefly. I am not going to take a lot of your time this morning in introductory remarks.

We would like to take some time to compare the core protection calculator system as it currently exists on Arkansas Nuclear One Unit 2 and that being proposed for San Onofre Unit 2 so you will have some base line for relying on our previous discussions on Arkansas.

That then would be a convenient point where I would intend to turn the presentation over to a representative from Arkansas Power and Light who is with us today. Arkansas Power and Light will give us the benefit of their experience in operating the core protection calculator system at ANO 2.

We would turn to the meeting back over to Combustion Engineering for a discussion of the software, the programming, the change procedures that we have used and are using, the changes which in fact have been incorporated into the system based largely on experience at ANO 2 and then we would turn the meeting back over to you for comments by the NRC staff on the review of the core protection calculators.

That is the agenda we have laid out for today and I think we can proceed expeditiously with that. If there are not problems with the agenda I would like to introduce our first speaker.

MR. KERR: Let's proceed expeditiously.

MR. KENNEDY: Our first speaker is Mr. Al Spinell from Combustion Engineering. Mr. Spinell is the Assistant Project Manager for our San Onofre Units 2 and 3 project at Combustion Engineering. Mr. Spinell will make a few introductory remarks on his objectives and then proceed to a description of the core protection calculators and a comparison of the Arkansas and San Onofre design.

Mr. Spinell.

PRESENTATION OF AL SPINELL

PROJECT MANAGER, SAN ONOFRE UNITS 2 AND 2 PROJECT

COMBUSTION ENGINEERING

MR. SPINELL: Thank you, Ernie.

Good morning gentlemen.

Let me make my remarks here stating our overall objectives for this meeting from this position and then I will move up and make my presentation formally using slides on the overhead.

Combustion Engineering has five objectives I think this morning or during the day's meeting that we would like to convey to the subcommittee and the consultants and they are as follows.

One, we would like to put in perspective the relationship of the CPC trips to the remainder of the plant protective system and to emphasize the backup features that exist in the remainder of the plant protective system which provide alternate protection.

Second, we would like to highlight the similarities between the ANO 2 design and the San Onofre design emphasizing that what we are doing for this nth plant, the San Onofre plant, is a relatively small extrapolation of the base line design.

Thirdly, we would like to provide an assessment of the CPCS behavior during the first one and a half years approximately of operation at ANO 2.

Fourth, we would like to demonstrate that a structured orderly process is in place for design and qualification of the software changes for San Onofre Units 2 and 3 and to identify how the ANO 2 experience over the last one and a half years has been factored in to the San Onofre software.

Lastly, Combustion would like to highlight the progress that we have made so far in the qualification process for the San Onofre software and its relationship to the licensing documentatior which we have prepared for the staff.

MR. KERR: That sounds like a reasonable approach and it also sounds as if you have a lot to cover. So the expeditious approach suggested by Mr. Kennedy is in order.

(Slide presentation.)

My presentation this morning will cover these four topics. What I intend to do first is to cover an overall description of the system. What I intend to do is not present any new information that has been before the subcommittee before but for new members present plus for the members that have been through the Arkansas review it will provide a refresher. I will speed through that process as best as I can striking an optimum approach of what I thought would be relevant here for purposes of the discussion.

Secondly, I would like to give a comparison between San Onofre Units 2 and 3 and the Arkansas designs.

Third, I want to provide a status of the overll system design qualification and field status of the equipment.

Fourth, I want to work in a summary statement with respect to our licensing status and the submittals we have presently into the NRC.

(Slide.)

The first several slides I have this morning deal with the concept of why we went to digital processing technology. I think they are embodied in three general design criteria for which I don't want to go into in detail but the first of which is general design criterion 10 of 10 C.F.R. 50, Appendix A which deals with the protection system requirements and margins required to preserve fuel design limits related to anticipated operational occurrences.

(Slide.)

These fuel design limits which we are relying upon are defined thusly for reference purposes, a linear heat corresponding to fuel centerline melt and the DNBR equal to 1.3 in the case for Arkansas and in the case of San Onofre Unit 2, 1.19 based on CE-1 correlation.

(Slide.)

This is the second of the three criteria. It embodies our philosophy regarding the core protection calculator system.

(Slide.)

And the third thusly.

(Slide.)

Now, over the years we found as well as relating our experiences within the industry and the NRC that there was a considerable discussion and changing opinions and attitudes about the interpretation of those criteria and based on our knowledge and experience in protection system design we felt there were reasons to make changes and the reasons therefor are embodied in the following two examples as I have listed here.

For example, with regard to single failures of an active component and inclusion of those as an initiating mechanism for an anticipated operational occurrence.

I cite two particular rod related events here which were not afforded direct protect by our protection system but in earlier days by control systems.

Secondly, I cite for example the case involving axial flux perturbations as might be caused by certain boron dilution events which were not embodied in part of our earlier protection system design.

(Slide.)

In order to accommodate those types of changes we felt that there was a potential need for make the protection system more responsive to these requirements.

The three things that we felt needed to be embodied in that upgrade of that protection system was that (1) we needed to sense the power distribution with increased accuracy, (2) we needed to include control rod position inputs in a discrete manner and, (3) we needed to provide increased direct line or on-line assessment of the thermal margin of the local power density characteristics dealing with the relevant cooling system parameters.

To more effectively implement this we came to the conclusion in the early to mid-'70s that digital processing technology as far as we were concerned could be incorporated into the plant protective system.

MR. KERR: Mr. Spinell, in your consideration of these operational features I think I understand the point you are making. I would appreciate your telling me, however, how you decided that these features to which you refer, for example, sense of power distribution with increased accuracy, include measured control rod position as input and so on should become part of the reactor protection system rather than, say, part of the reactor control system.

In a sense you are talking about handling the plant in situations which are anticipated to occur during the life of the plant. So that although they are not perhaps the day-to-day oerational events, they are events which you expect to occur and which hence the plant needs to be able to handle.

How did you decide that the handling of these should be the responsibility of the reactor protection system rather than the responsibility of the reactor control system?

MR. SPINELL: Let me try and cite an example that deals with the rod drop event. In our early plant designs initially we typically afforded an overpower margin in the plants that would accommodate a rod drop event. That overpower margin typically was substantial, i.e., it would potentially penalize the plant capability in terms of operating flexibility, but that was a given tradeoff.

In order to handle that kind of an event we provided not only that overpower margin but we had features in the control system in the secondary plant that provided turbine run-back capability to minimize the mismatch between the primary and secondary system.

During various reviews by the staff as well as ourselves regarding that type of an event, and it was categorized as an anticipated operational occurrence. If you will refer to the appendix in the general design criteria it is defined as occurring once or more in the 40-year lifetime of the plant.

We sensed an increasing need either to design more appropriately that control system feature where we had more rod block, if you will, as well as rod runback, or as an option to put in some automatically responsive redundant single failure proof feature in the plant protective system proper which could accommodate that rod drop event automatically. One way to do that would be to have the protection system have in a sense discrete rod inputs on line.

MR. KERR: Mr. Lipinski.

MR. LIPINSKI: On Turkey Point you had implemented the linear heat rate and the DNBR via analogue computers, but, if I recall, you did not have the ability to sense the rod positions. So you are taking the penalty on Turkey Point.

MR. SPINELL: Are you referring to St. Lucie?

MR. LIPINSKI: I am sorry, St. Lucie.

MR. SPINELL: Yes.

MR. KERR: Let me see if I understan the import of your comment. I could interpret it to mean that having recognized that you needed to handle these infrequent but nevertheless expected during the life of the plant events and having concluded that the reliability of the system needed to handle them possibly because of their consequences or whatever was something that needed to have some quantitative significance like the single-failure criterion and a qualitative significance perhaps you decided that the way to get that would be to build a system which would have the characteristics now attributed to protection systems, namely, redundant channels, single-failure criteria and so on. And having made that decision that it must meet the criteria of a reactor protection system it sort of became part of the reactor protection system.

MR. SPINELL: That is correct.

MR. KERR: Let me ask one other question. You have referred to the general design criteria of the NRC as background for general guidance I guess in deciding how to design. Does Combustion Engineering have any similar set of criteria that may be similar or perhaps independent of the general design criteria of NRC?

MR. SPINELL: Bill.

MR. GILL: My name is William Gill from Combustion Engineering. I don't think we really have any different criteria. I believe our interpretation of the criteria varies somewhat from industry interpretations. As designers we are more sensitive to certain issues like operator actions.

As Al was pointing out in the CEA misoperation we relied on control systems but we also relied on the operator to trip the plant. At the time we were making the decision to go to the core protection calculator we interpreted the criteria such that operator action would only be appropriate if you had a clear unambiguous indication of the process and if you had sufficient time to implement that action. So I don't believe our criteria are different but it is just our interpretation of the criteria.

MR. KERR: That comment is relevant. I also had in mind the possibility that you might have specific criteria for performance of control systems. NRC's design criteria are much less applicable to, say, determine reliability of control systems and, as I understand the argument, this philosophy is based on the assumption that the combined design of control and protection systems is such that the reactor protection system bears the burden of whatever reliabilty one enforces.

Now, it is not obvious to me that a nuclear steam supply designer would have the same approach and I wondered if, for example, you have design criteria which perhaps you apply to control systems, reliabilty criteria, for example?

MR. GILL: I will answer your question in a time frame. At the time we made the decision to implement the digital protection system and during the design process which was in the mid-'70s to, say, 1978 the answer is no, we didn't put the rigor into criteria for control systems that we did for protection systems.

MR. KERR: Excuse me. I didn't mean to imply that you would have the same ones. I just wondered if you had any?

MR. GILL: At that time they were minimal. I think at the present time we are developing criteria for the reliability and failure of control systems. This is primarily prompted by their impact on plant availability. That is our initiating mechanism for looking at it.

In developing these criteria though we do find that there is a link between the control system reliability and the protective system design criteria and that if we de. lon criteria for control systems and design those control systems to that criteria then your failure modes or their reliabilty is much higher and the potential for failure is much lower.

In this case we could move certain events say from anticipated operational occurrences to say anticipated accidents would be a lower probability event. This in turn would relieve some of the say pressure or some of the requirements on the protection system.

So that development of crite.ia for the control system is something that is underway but it is at the very early stages of development.

MR. KERR: Any estimate of when you will have those criteria developed? I presume they never become fully developed because as you have learned they may change.

MR. GILL: I can't give you the calendar time but I can give you the process by which we would hope they would become developed. CE has recommended and is working with various industry committees to try and establish say an IEEE A&S Committee on Classification of Instrumentation where we would develop the various classes of instrumentation.

Once we developed the classification we would then develop criteria for each class. This would include control systems and safety systems and in all likelihood it would also break the safety systems into two pieces, safeguards type protective sytems and reactor type protection systems which could have different criteria.

Our intent would be to approach this as an industry effort rather than CE approach it by themselves and we are working toward that goal.

MR. KERR: So when you tell me that development is underway you are referring to an industrywide effort carried on, for example, by an IEEE committee?

MR. GILL: We as a designer are proceeding with that criteria. Our incentive to implement a criteria like that as a sole designer of power plants is not that high. It has a significant impact on our, you know, position in the industry to be the only one to impose a criteria on control systems unless we can convince ourselves that the benefit of doing so, you know, is significant.

MR. KERR: It is hard for me to see how one could fail to be convinced that control system reliability would be an asset. How does one avoid such a conclusion?

MR. GILL: Control system reliability is an asset.

MR. KERR: Mr. Ditto.

MR. DITTO: I hear about the control system reli bility and I think of an equally important part of the control system and that is its performance capability. I think part of the reason for going to a different kind of protection system, an improved protection system is the fact that your control system was not capable even when it worked of assuring sufficient margin. That is, you could not reduce the margin enough because your control system did not take into account rod position in a way that let you be assured that your protection system would be adequate without putting in a great deal of margin.

So I think when you develop these criteria they must include as well as reliability a very strong concern for the capability to keep the plant in an ideal state if you please when it is working.

MR. GILL: I think you are addressing two issues. The control system can maintain the initial conditions for the accident. The control system can also reduce the probability of the event.

MR. DITTO: Certainly.

MR. GILL: However, once the event is initiated, if that event left uncorrected could result in violation of fuel design criteria or plant design criteria, then it must have a safety system in terms of the redundancy, reliability, et cetera.

MR. DITTO: Certainly.

MR. GILL: So our decision as to whether we use a control system or a safety system is pretty simple. If the process proceeds without mitigation and that process would result in violation of either the fuel design criteria, pressure boundary or containment design criteria then a safety system designed to the IEEE 279 criteria, et cetera, is required to mitigate that event.

MR. DITTO: Yes. I was only trying to make the point that if your control system does not have the capability even when it is working of maintaining the plant in a state that your protection system can mitigation if it gets into the accident condition then the reliability becomes not very much of an issue.

MR. GILL: Correct. Let me just point out one thing. We rely on the control system to maintain the overall process. However, we rely on monitoring systems such as our core operating limit supervisory system and other systems to maintain the plant within the initial conditions in the accident.

So there is really a level of control system that is say one notch up in terms of criteria which maintains the plant consistent with the initial conditions in the safety analysis. CE has developed criteria for the design of that type of system. For example, we apply certain aspects of QA to those systems.

MR. KERR: Mr. Lipinski.

MR. LIPINSKI: In the case of the rod drop accident if you were to employ a rod runback rather than a scram is there sufficient time to guarantee that you do not exceed the core limits or must you scram?

MR. SPINELL: I think it depends on the conditions.

MR. GILL: Sir, are you asking is there sufficient time for operator action to trip the reactor?

MR. LIPINSKI: No, no. I am talking about an automatic rod insert as opposed to a total reactor scram. Let's say I have a rod drop accident. If I were to employ a rod runback do I guarantee that the fuel design limits are not exceeded or is the time such that I must employ a scram?

MR. GILL: You must employ a scram.

MR. LIPINSKI: Okay, that answers the question. You really can't protect against this type of an event with a control system action. You must employ scram.

MR. GILL: On the Arkansas and later plants, the high-power density plants and the large cores that is true. On the operating reactors there is more time and sufficient time that a trip is not needed. It depends on the margins in the plant.

MR. LIPINSKI: That is what I was going to comment on. If you do not employ the fast ground then you have to increase the margins such that the fuel limits are not exceeded.

MR. GILL: That is correct.

MR. KERR: Mr. Ray.

MR. RAY: Referring to criteria reliability do you have any performance standards which you require your computer system component suppliers to demonstrate such as mean time between failure of components and that sort of thing?

MR. KERR: Mr. Ray, are you referring now when you say "computer" to the core protection calculator computer or the plant computer?

MR. RAY: You said digital processing technology was incorporated into the PPS. I am talking about that digital computer technology, the systems that are involved.

MR. KERR: Do you understand the question?

MR. GILL: We will be discussing that in some detail at later parts of the presentation. So if you don't object we would like to put that off and we will be getting into reliability.

MR. RAY: No objection.

MR. KERR: Okay.

MR. GILL: Dr. Kerr, if I could just add one more item on the control system. The implementation of the protection system for CEA events was a licensing condition for Arkansas. It was part of the PSAR safety evaluation report. Its safety grade rod protection must be incorporated in the plant. There was an alternative for analysis but that alternative was not viable.

MR. KERR: Thank you.

Mr. Lipinski.

MR. LIPINSKI: That last one leaves me confused because St. Lucie was licensed without it, right?

MR. SPINELL: St. Lucie Unit 1; that is correct.

MR. LIPINSKI: So now what happened between St. Lucie and Arkansas that required that you use the rod information and generate a scram?

MR. GILL: Reinterpretation of the criteria on St. Lucie.

MR. LIPINSKI: By NRC or Combustion?

MR. GILL: I would say by both. The staff issued a directive that said a safety grade rod block is required on the Arkansas plant. CE was involved in criteria that limited operator action if that action were required in short periods of time. Trying to decide who got there first and impose the criteria is very difficult. Looking back I would say it was an overall industry interpretation of criteria imposed by the NRC.

MR. LIPINSKI: Thank you.

MR. KERR: Any other questions?

Please go ahead.

(Slide.)

MR. SPINELL: This slide, what I want here to do is to convey in the proper perspective the relationship between the plant protective system and the core protection calculator trips.

The plant protection system as defined consists of two basic components, an engineering safety features actuation system and a reactor protection system.

The core protection calculator initiates two of the twelve trips in the reactor protection system portion, the low DNBR trip and the high local power density trip for San Onofre Units 2 and 3. They are represented here pictorially. There are ten other analog type trips, typical trips that are consistent with Arkansas as well as our other earlier plants. In addition, there are seven analog safety functions for actuating emergency safeguards such as ECCS.

MR. KERR: I hate to introduce a discordant note into your presentation but remind me what SONGS means.

MR. SPINELL: San Onofre Nuclear Generating Station.

MR. KERR: I was afraid of that.

(Laughter.)

(Slide.)

MR. SPINELL: For these two trip functions and the relationship between the remainder of the protection system I have this slide. The point I want to get across to you is that given the fact that we have undergone an extensive review of this system and given the fact that we have put a lot of time and effort into it the relationship of the core protection calculator to the remainder of the system is such that even with a diverse common mode, if you will, failure of all of the four redundant channels in this computer system an evaluation has been performed.

We have come to the conclusion that we have event specific backup trips, diverse analog trips that are embodied within the remainder of the protection system and these I have listed by event and have listed the backup trip that is implemented at San Onofre.

MR. KERR: Excuse me. I guess I am not altogether certain of the significance of your statement. Is the significance that even if the CPC were obliterated you would still be able to take care of trips for most of the events of which you can conceive?

MR. SPINELL: That are part of the present design basis for the CPC, yes.

MR. KERR: I am sorry. Would you repeat that.

MR. SPINELL: I have a later slide which defines the individual design basis events and these are categorized accordingly. The answer to your question is yes, there are backup trips.

MR. KERR: Thank you.

Mr. Ray.

MR. RAY: Are these backup trips part of the computerization or are they an entirely independent system?

MR. SPINELL: They are part of the analog portion of the reactor protective system.

MR. RAY: They are not then an independent channel within your CPC system? They are completely independent of any computer component?

MR. SPINELL: They are completely independent of the CPC channels.

MR. RAY: You said you had four redundant channels within the CPC system. What happens when one of those malfuntions and goes out? Is it automatically switched or must an operator intervene to switch over to the other channels?

MR. SPINELL: Well, there are two principal ways, if I can use your term, that a channel goes out. One, it can automatically trip or the operator can take it out of service for a periodic testing, maintenance or whatever.

In the case of the first obviously the function is an automatic trip of that channel and that provides part of the coincidence logic for tripping the reactor. There needs to be two like channels to provide that trip function.

In the case of the latter the operator can simply take the channel out of service at the appropriate panel and perform whatever maintenance or testing functions he has to to meeting the technical specification requirement. He then has the other three channels in this case to provide him the necessary protection which meets the criteria.

MR. LIPINSKI: May I add to that statement. Channels can fail two ways, unsafe or safe. If the safe failure occurs then one channel has failed and that is a two out of four system. Any one of three remaining channels provides a trip if an event occurs. If it is an unsafe failure then that system reverts to a two out of three system and then you require two channels to come up to generate to trip.

MR. RAY: So you don't necessarily have a half scram situation.

MR. LIPINSKI: No, no. The scram goes to completion if it comes up but based on the two out of four. If it unsafe you revert to two our of three. If it is a safe failure then it is one out of three.

MR. RAY: Another question. Does the system have any self-diagnostic capability so that when one channel fails the computer diagnostics can take over and tell the operator possibly which component in that channel failed or must this be an entirely separate investigation?

MR. SPINELL: Depending on the set of circumstances there can be immediate indication of the cause of the problem or under certain circumstances the operator or the technician might have to take a channel out of service to perform some diagnostics. He can do that by interrogating the components.

MR. RAY: So there is a partial self-diagnosis in your design?

MR. SPINELL: That is correct.

MR. KERR: Mr. Ditto.

MR. DITTO: I presume there are cases in which you could have failures that are there lying dormant which you don't know about and may not even detect during tests.

MR. KERR: I am sorry, you could have what lying there?

MR. DITTO: Failures, component failures or system failures in channels that you don't get at by any of these methods. You can have a channel out of service for particular accidents in a way that you don't know about, senses that have failed in some peculiar way. Your diagnostic is of the computer system and it is not of the entire system.

MR. KERR: Is that a statement or a question, Mr. Ditto?

MR. DITTO: I am asking him is that not true.

MR. SPINELL: There are separate diagnostic procedures, and I will let Arkansas if they are willing to address that, introduced for the processing equipment upstream of the core protection calculators specifically for the sensors themselves, the transmitters and the processing equipment, response time testing, et cetera, that determine the operability or status of that equipment.

MR. KERR: Mr. Lipinski.

MR. LIPINSKI: One of the purposes of connecting the Arkansas CPC's to the plant computer was to use the plant computer to do an interchannel comparison and to sound an alarm if there was a deviation on any single channel compared to the others. Right now you don't have the intercomparison capability, do you? I am askin it of him.

MR. KERR: He is not Arkansas.

MR. LIPINSKI: No, but he was involved with the design of the system.

MR. SPINELL: Can you repeat the question again, please?

MR. LIPINSKI: The purpose of interconnecting the Arkansas CPC's to the plant computer was to use the plant computer to do an interchannel comparison on the CPC's and to sound an alarm if there was a significant deviation of any one channel from the average performance. That connection was not allowed to be made and consequently you are not performing those intercomparisons.

MR. SPINELL: Let me have Mr. Cogborn from Arkansas Power and Light address your question.

MR. COGBURN: My name is Thomas Cogburn.

Regarding the data links from the core protection calculators to the plant process computer the resolution that was agreed upon at the time of licensing of ANO 2 was that at the completion of the start-up test program plus ten days the data links would be removed.

Prior to that time, prior to completion we sent a letter to the NRC staff asking concurrence that we leave the data links in service. Because we received no response to that letter we took it as concurrence and we still have them installed and we are using them now.

MR. LIPINSKI: Thank you. I wasn't aware of that. I knew the first one was in force but I didn't know it never was implemented.

MR. KERR: Mr. Ditto.

MR. DITTO: I have to say one thing here about this. It is my understanding that the use of redundant channels is so that each of four or three independent channels can tell the protection system what it thinks the status of the plant is.

In this intercomparison that is easily done with a computerized system you somewhat sacrifice this independence and you lead people into the notion that agreement among these channels is a good thing. I suggest that agreement among protection channels to a very close comparison is probably not a good thing to insist upon. So I just throw that in as one of the hazards that you have of making this easy intercomparison that you somewhat lose the independence of the channels in a rather subtle way.

MR. KERR: But very, very subtle. It is so subtle that I have never understood it.

MR. LIPINSKI: I was going to ask for him to amplify it because now it is a fifth computer that is the referee.

MR. DITTO: Which has only one set of inputs or a number of them.

MR. KERR: You and Walt and I will have to go out in the hallway and debate this further. Let's continue with the presentation.

(Slide.)

MR. SPINELL: In the next series of slides I would like to define the CPC scope, the hardware, the software, the inputs and the outputs.

The first of these slides introduces the scope of the system and it embodies the following four items.

First, signals from sensors that m[illegible]or specified core variables, and I will define those variables in a later slide.

Secondly, dedicated computers, a total of six divided up into four channels, to implement the algorithms that will process the sensor information.

Thirdly, operators' modules for visibility indication.

Fourthly, outputs for displays, alarms and reactor trips.

(Slide.)

The next two slides I have in a package. They are in reversed order if you will bear with me.

What I would like to cover in the next two slides is a definition if you will of the design basis for the system as it is presently embodied. This is an overall design requirement in that it covers certain anticipated operational occurrences and design basis accidents.

In the first with regard to anticipated operational occurrences the system is designed to provide or to initiate automatic protective action to preserve the margin present to assure that we will not violate the fuel design limits specified earlier on fuel centerline melt and DNB.

Secondly, the core protection calculators for a fixed finite set of design basis accidents coupled with certain engineered safety features actions help to assure that the consequences of those accidents are within the analysis results that have been computed.

(Slide.)

The specific design basis events within those two categories on your previous slide are identified thusly. In the anticipated operational occurrence category Xenon oscillations are included in the protection as well as the rod-related events listed, excess and loss of load functions on the secondary plant, complete and partial loss of forced reactor coolant flow in the primary system, uncontrolled boron dilutions initiated by manual misoperations or failures of equipment in the chemical and volume control system and asymmetric transients that perturbate one side or another of the reactor coolant system via the heat sink.

In the accident catetory the core protection calculator provides protection for the steam generator tube rupture and reactor coolant pump shaft seizure events.

MR. KERR: Mr. Spinell, what is meant by steam generator tube rupture as an accident? Does that rupture of one tube or several tubes? How much of a rupture does it have to be in order to put it into the accident category?

MR. SPINELL: Any partial or total rupture which causes a loss of coolant rate that exceeds the make-up capability of one charging pump which is 32 gallons per minute.

MR. KERR: That is really in terms of leakage?

MR. SPINELL: Right.

MR. KERR: Thank you.

Mr. Pearson.

MR. PEARSON: Let me ask you a question. When you say an uncontrolled Xenon oscillation does that implying that a control system has failed to operate?

MR. KERR: Do you understand the question?

MR. SPINELL: Yes. I would like to call on Bill Gill to handle that question.

MR. KERR: Mr. Gill, did you hear the question?

MR. GILL: No, I am sorry. Could you repeat the question, please.

MR. PEARSON: When you say you have an uncontrolled Xenon oscillation does that imply that a control system has failed to operate?

MR. KERR: Mr. Pearson is referring to the first of these listed.

MR. GILL: Yes, sir. No, it does not. We do not have automatic control of axial power distribution. The large cores, the Arkansas core and later are predicted at certain times in life to be unstable. In other words, the oscillation will diverge. It is the responsibility of the operator to control that Xenon oscillation and bring it back to a stable nonvarying condition. Should he fail in doing that then a protective system would initiate a trip.

MR. KERR: Thank you.

Please proceed, Mr. Spinell.

(Slide.)

MR. SPINELL: Let me then highlight with this slide the design features that we have incorporated in the core protection calculators to provide protection.

First, included in the system is a set of fourfold redundant three-level ex-core detector information. These are vision chambers, three separate vision chamber assembles located outside the reactor vessel segmented into four separate channels.

In addition there is a complete system of dedicated digital computers to provide this four-channel redundancy.

There is the use of analytical synthesis techniques to construct radial and axia` power distributions on line.

Fourth, the use direct CEA position inputs based on rod positions.

Next, flow determination based on direct reactor coolant pump speed measurements based on revolutions of the shafts of the pumps individually turning.

There is linear heat rate and DNBR calculated on line in the system.

Lastly, an operator's console channelized to provide a comprehensive data display that the operator can interrogate via keyboards.

MR. KERR: Full determination based on RCP speed measurements. Is that a one-for-one correlation or is that based on RCP speed measurements plus some other things?

MR. SPINELL: In a static sense the process input is a direct speed measurement based on a probe assembly that sits around the shaft. The probe measures the revolutions by monitoring a discretely defined set of grooves or discs within that assembly. The proportionality of the speed of the shaft turning with the number of counts, if you will, that probe assembly picks up as the individual indicators around the probe shaft turns is the input which is then converted into individual flows based on the individual pump head curves for this particular system.

MR. KERR: As I recall, and I haven't looked at the CPC in a year or so, that measurement was then modified somewhere in the calculation to come up with a corrected flow. That is, if my memory serves me correctly, there was some kind of a fudge factor, if you please, that had to be applied farther down the lin- in the calculator.

You are saying that the head characteristics of the pump and the speed is all that goes into the flow calculation?

MR. SPINELL: I might call on again Bill Gill who can address that in a dynamic sense of how those flows are compensated.

MR. GILL: In terms of the on-line calcultion in the CPC you can look at it as a flow algorithm. In the inputs, in terms of measured inputs to that algorithm are pump speed, system pressure and system temperature, the pressure and temperature being density, friction factor type of corrections which are used in a flow calculation.

That basically allows the calculator normalized flow. That flow must be calibrated to an off-line determination of flow rate using a combination of pump DP instrumentation and a heat balance on the primary side to determine the absolute value of flow. That absolute value of flow becomes a calibration factor which is entered into the core protection calculator by the addressable constance technique which are adjustment factors.

MR. KERR: Thank you.

Please continue.

(Slide.)

MR. SPINELL: This next slide depicts a representation of the relationship between the calculators and the rod position inputs. I might point out at the beginning that the remainder of the process inputs that are displayed on the next line are not shown in here for each of understanding but on an individual channel-by-channel basis across for the four redundant core protection calculators there are also inputs for primary pressure, temperatures, shaft speed sensing inputs and ex-core detector information that are input functionally into the calculators here.

I might draw a line here and show these inputs. Those are other process inputs.

If you start at the top of this diagram here there are 91 CEAS in the San Onofre Units 2 and 3 design. Each of them has two separate redundant reed switch position transmitter assemblies that provide discrete position input into the core protection calculator system.

There are 23 target rods, if you will, based on the group and subgroup assignments that are input into the individual core protection calculators which provide group relationships to one another and identify certain peaking factors to those relationships, if you will, if the groups are separated more than a particular amount.

In addition, all of the rod position inputs for individual groups are provided in the core element assembly calculators. All 91 reed switch position inputs are in each one of these calculators and these provide individual CEA deviation information that has thus input into each of the core protection calculators via data links. These data links are isolated to maintain their proper separation.

In addition, the output of each of the control element assembly calculators, CEA calculators, are isolated and input into a CRT display on the control board that the operator has the capability to obtain the information from either of the two calculators.

One other point I would like to make with this slide is that at the present time the data links that we were referring to earlier today, the output, if you will, from each one of these calculators goes to the plant monitoring system, and I will draw in the other lines for detail, that provide all of the information for the interchannel comparisons and the information that is used during the power essential test program for verification of various constants in parameters.

(Slide.)

The next slide depicts the process input signals and all of these were, as I pointed out, not represented explicitly on the previous slide with the exception of the target CEA position information. This slide depicts the signal itself, the number per channel, the range of the individual parameters and the signal types.

(Slide.)

To define the inputs to the system of hardware itself then it is appropriate to define the algorithms themselves that the calculators process with this process input. They process four major application programs in addition to a trip sequence program to identify to the plant protective system the trip sequence necessary.

The four basic application programs are the coolant mass flow program, the DNBR and local power density update program, the power distribution program and the static DNBR program.

(Slide.)

The major calculations within the system are broken out in a little more detail for the four particular programs involved.

First is the Flow Program. It calculates mass flow rate in the system and it determines a projected DNBR based on a projected change in the flow rate itself. As Bill Gill identified, this information is compensated by temperature and pressure inputs with respect to the effects on density.

The second program, the Update Program, determines the partial derivative, if you will, updates of a series of parameters with respect to their impact on local power density and DNBR, in particular temperature effects, pressure effects and so on.

(Slide.)

The third program, the Power Program, is basically a Delta P power program calculation, if you will, that uses these inputs.

The fourth program is a Static Program or a static computation of DNBR and local power density which uses the major types of information identified here.

(Slide.)

So we have talked about the hardware itself, the process inputs, the application programs and these are the output signals from the calculators on a per-channel basis.

In addition to the normal DNBR and local power density trip information we have pre-trip indications, we have output signals for sensor failures, we have information dealing with mass flow rate and calibrated neutron flux.

The signals that I have identified thusly are here, the types involved, whether it be contact or analog information, the setpoint where appropriate and then the range of the particular signal where appropriate.

MR. LIPINSKI: Before you take that off, on that range column the DNBR margin to trip, zero to ten, does this mean you can make a dignital entry of ten as an analog setting? Is that the upper scale for a trip on DNBR, ten?

MR. SPINELL: Let me ask Bill Gill or Ed Brown to address that.

MR. GILL: That is the scale on the analog output. It is a zero to ten volt signal, and zero to ten volts corresponds to zero to a ten DNBR margin where a zero margin is a trip and a ten is a calculated DNB of ten plus 1.3 or 1.19. It is just a scaling factor.

MR. LIPINSKI: I know it is a scaling factor. What I am getting at is normally you are talking about levels of 1.3 and normally you are set in the vicinity of 1.3, are you not, for your trip?

MR. GILL: Correct.

MR. LIPINSKI: But you are telling me that if I were to be an operator I could run that dial up to ten?

MR. GILL: No. That is the calculated output and not the setpoint. The setpoint is basically a digital word in memory. That is the analog output which goes to an analog meter.

MR. LIPINSKI: Correct. So now what does range mean zero to ten on that analog meter?

MR. GILL: It means that the calculated margin can be zero to ten DNB units which corresponds to the full scale on the meter. If you look at the face of the meter in the control room it would show zero margin which would be a trip condition and then it would go up to ten. When the reactor is starting up say at ten or fifteen percent power you would see that the DNBR margin would be up around nine or ten and it is scaled so that the operator can observe its performance during start-up and assure that the system is functioning.

MR. LIPINSKI: You are telling me your scale is not related then to the actual DNBR? I would normally expect to see numbers like 1.3. What do I interpret when I see a number of ten?

MR. GILL: What is displayed to the operator is not the calculated DNB. It is the calculated DNB minus the setpoint. So it is the margin to trip where zero margin means that he is at the trip setpoint of 1.3. We are showing him on an analog meter the margin he has in DNB units. So a reading of ten would mean that he has ten DNB units to trip.

MR. LIPINSKI: 1.3 minus 1.3 is equal to zero.

MR. GILL: Right.

MR. LIPINSKI: 1.3 minus 1.2 is .1.

MR. GILL: Right.

MR. LIPINSKI: Where do I get ten?

MR. KERR: If your ratio is 11.3 you get ten, Walt.

MR. LIPINSKI: Okay.

(Slide.)

MR. SPINELL: For completeness within the system let me show our next slide, the program execution intervals and the sampling rates for the inputs by programs listed here, the four major programs, the inputs sampled by program and the execution or sampling interval.

The note down here dealing with the display of the information on the operator's console which, depending on the input, is some many times after a particular sampling frequency adjusted accordingly.

In this case the execution and sampling interval for the programs is consistent. There is a one-to-one correlation between the sampling and the execution of the program.

(Slide.)

This next slide will leave you with the impression that there is ample information displayed to the operator by various means within the control room not only via the operator's module which receives a lot of attention and the displays which have these features, but also the direct analog indicators that are provided on a channel basis for each of the three functions listed.

In addition, there are inputs to the station annunciator system for a pre-trip and trip alarm indication.

In addition, there is individual process information on each of the process inputs to the system that is displayed on the control board.

Last, there is the CRT display for the discrete rod position input or on a bank or subgroup basis. In fact we have 91 control rods here listed instead of 81.

What I would like to move now to is a comparison of designs between the ANO 2 system and the San Onofre Units 2 and 3 system.

MR. KERR: Mr. Spinell, this strikes me as a good point for a break. If you agree I will declare a ten-minute break.

MR. SPINELL: All right.

(Whereupon, a brief recess was taken.)

MR. KERR: Are you ready to begin, Mr. Spinell?

MR. SPINELL: Yes, I am, Dr. Kerr.

MR. KERR: Okay. Let's get started.

MR. SPINELL: For this portion of my presentation I want to provide a comparison between the San Onofre Units 2 and 3 and Arkansas designs with respect to these three categories: First the hardware, next the executive system software and the application system software.

(Slide.)

For the sake of the hardware comparison after you read through all of this what we are basically saying is there are no hardware changes or, in other words, the systems are identical hardware-wise between San Onofre and Arkansas.

It so happens that we have different cable lanes for some of the interconnecting equipment and we have additional spare cards that handle the additional rod position inputs. It so happens they appropriately accommodate the increased number for San Onofre. But the hardware, the vendors, the design of the hardware is identical. In fact, they were made out of the same lot at Systems Engineering Laboratories at the same time.

(Slide.)

The next slide is a comparison with respect to the executive system software. As pointed out here there are no differences in the software design between the two systems, including the following functions dealing with task scheduling, priority and software structure of the programs.

As pointed out here since the two plants have different numbers of control element assemblies, 83 in Arkansas versus 91 in San Onofre, the programs that service the various input and output data dealing with that are adjusted accordingly to accommodate those additional CEA positions.

MR. LIPINSKI: What are the exact numbers of CEAs?

MR. SPINELL: Ninety-one on San Onofre and 81 on Arkansas.

MR. KERR: So the numbers are 92 on San Onofre and 81 on ANC 2?

MR. SPINELL: Correct.

MR. KERR: Thank you.

(Slide.)

MR. SPINELL: The third of the last three elements of this comparison deals with the application programs and the difference in the programs between the presently configured installed software in Arkansas and the pending completion of the cycle one software for San Onofre. They are embodied in these changes thusly dealing with the DNBP algorithm itself where we are going to the torque CE-1 thermal hydraulics code correlation methodology for determining static DNBR. There are assorted data base changes to reflect plant specific cooling system characteristics and related power distribution information.

Thirdly, there are CEA related changes dealing with the numbers of rods, the penalty factors, et cetera.

MR. KERR: Mr. Spinell, help me a bit. In the previous slide I saw that there were no differences in the software design and in this slide I find that there are differences in the algorithms.

Now, I presume what you are saying is that there is no difference in the software design but there is some difference in the software. Is that the way I interpret those two slides?

MR. SPINELL: Dr. Kerr, the previous slide could have been clarified by saying an executive software design or executive system software design in lieu of software design as a point of clarification.

MR. KERR: That refers only to the following executive system functions, whatever that means.

MR. SPINELL: Correct.

MR. KERR: Okay. So there are some differences in the software between the two systems?

MR. SPINELL: In the application programs, correct.

MR. KERR: Okay.

MR. SPINELL: One more point I would like to make here is these changes that are undergoing implementation on San Onofre Units 2 and 3 are planned to be implemented in the cycle 2 software for Arkansas Power and Light.

MR. KERR: Is somebody going to discuss the reason for those changes and the implications thereof?

MR. SPINELL: We will be getting into those changes in a session in the afternoon as far as that goes.

MR. KERR: Thank you.

(Slide.)

MR. SPINELL: The third item I would like to give you an overview on this morning is a status of the design, qualification and field activities dealing with the system on San Onofre for purposes of having the perspective on where the basic elements of the system stand at this point.

The first four items on your list here deal with the hardware principally.

I might point out, first of all, that the hardware design was completed approximately in August 1976. The hardware was completely fabricated and delivered and installed to the site and that activity was completed in approximately June of 1978.

In approximately October of 1980 the actual base line field acceptance test on the hardware was performed.

At that time the system was initially energized with the proper uninterruptible power supply filtered appropriately to meet the requirements. In fact, that is a benchmark test, if you will, for warranty and other purposes.

Since that time we have initiated the field preoperational test on the system which includes various continuity checks on the process inputs. We have tested software in the calculator system itself to determine electrically that the system functions properly.

The remaining activities that we have to perform on the system itself are a set of tests which include prior to fuel load response time testing on the equipment and just as importantly during the post-fuel load phase a series of tests to measure and monitor the inputs and outputs of the system as well as various constants and data base inputs and a series of tests during the power ascension test program at the various plateaus.

The additional activities that we have going on in parallel right now dealing with the software include the following, the functional design activities of the software. If you will, the description of the final form of the algorithms to be implemented in cycle one for San Onofre was completed earlier this month with the release of appropriate functional description documentation.

In addition, we are approximately 90 percent complete at this time with the data base documentation for the over 5,000 constants that are a part of those application programs in the software.

In addition, we are proceeding and are about half way towards completing the software design process, the actual final flow charting and software implementation, if you will, via the programmers of the functional description forms of the algorithms.

Lastly, we are initiating efforts that are approximately five percent complete on the software testing phase of the work which would be completed approximately in April of this year.

The major effort now in that phase is defining the ensemble of test cases and the initial test conditions for those series of statis and dynamic tests that are to be performed that qualify that software.

MR. KERR: Let me see if I understand the relationship between 7 and 8. Seven says that the software design is about 50 percent complete and should be completed in March or '81?

MR. SPINELL: That is correct.

MR. KERR: And eight says that the software testing will be finished or that the design of the test will be finished in April of '81, which?

MR. SPINELL: We intend to complete the testing in

April 1981, two months hence.

MR. KERR: That strikes me as being a remarkably accelerated schedule, but sobeit.

MR. SPINELL: The actual program, and we will be getting into this in a little further detail later today, is such that with the methodology in place and with the test system in place what we need to is to complete a definition of and the boundary conditions for the test cases and actually test that software.

The actual fundamental turning of the crank to run all these test cases is an uncovery process of two or three weeks. So we believe it is a realistic schedule under these circumstances.

MR. LIPINSKI: When did ANO 2 go operational?

MR. SPINELL: Tom.

MR. COGBURN: The operating license was received on July 18th of '78.

MR. LIPINSKI: When did you get the power?

MR. COGBURN: Initial criticality was December 5 of '78 and the power operation continued in testing throughout '79. I will be describing that in a little more detail.

MR. LIPINSKI: Now, on this list you are showing that you had a field hardward acceptance test, and since you are working on the software naturally there was no software test. But with ANO 2 you had your software tested offsite before the equipment was installed, did you not?

MR. SPINELL: That is correct.

MR. LIPINSKI: So in this case you won't have a systems test until that software is completely developed and loaded into the onsite computers.

MR. SPINELL: We will have a system test on the Windsor single-channel facility via complete channel of hardware with the software integrated accordingly.

MR. LIPINSKI: Okay. So that facility is still available to you for development purposes.

MR. SPINELL: That is correct.

MR. LIPINSKI: And we are going to talk about these tests in detail as part of this afternoon's schedule?

MR. SPINELL: We will be talking in more detail about the whole change procedure methodology which a part of that embodies the actual test program, the qualification program.

MR. LIPINSKI: And you will detail the tests themselves in terms of the inputs that you are going to generate?

MR. SPINELL: We will be able to discuss that.

MR. LIPINSKI: Okay. Thank you.

(Slide.)

MR. SPINELL: The fourth topic that I would like to talk about briefly this morning and to wrap up my presentation covers the licensing status from our perspective at this standpoint. It embodies three elements in summary.

One, the extent of compliance with the 27 NRC staff positions on the core protection calculator system that were identified during the Arkansas review.

Secondly, the SER open item, the safety evaluation report item that is currently identified in the NUREG document issued earlier this month.

Thirdly, other what I might categorize relevant issues to the CPC review.

(Slide.)

With respect to the 27 staff positions the San Onofre Units 2 and 3 design, and not 1 and 2 as listed there, is in full compliance with the 27 positions with the exception of the position taken by the staff with respect to the data links between the calculator system and the plant monitoring system and Edison position I have listed thusly at this point.

MR. LIPINSKI: Let me ask this question. In the case of Arkansas it was silence that allowed those links to be maintained. What is the situation on San Onofre? Has the question been asked or are you proceeding on the basis of the Arkansas silence?

MR. KERR: I think that question probably ought to be asked of of the NCEP people rather than CE.

MR. LIPINSKI: Well, it probably should be asked of the staff.

MR. KERR: Well, maybe you should ask both, but I doubt if CE wants to answer that question.

MR. EPLER: I would like to raise a question in that area and it may be fundamental. After having observed 35 years of experience of operation it turns out that we never see a case where one with four redundant channels fails and nobody does anything and then another one fails and nobody does anything and we get demand and we have a system failure. It has never happened.

I don't think it ever will happen because we have claimed I think correctly that we have a test procedure to discover failure and we discover it and we do something. If they fail every day we have got a pile of junk. If they fail once a year we can handle this and we do handle it.

But if you look at the experience what we discover is some idiot turned off the protection and started an excursion and we had an accident. Maybe the designer did it and we have had cases where the designer did, where the operator did and where the excursion itslef has knocked out the protection.

Now, armed with this knowledge that the failure mechanism is not to be discovered by interchannel comparison but has to be looked at on the basis of somebody has turned off the protection that initiated the transient then I would ask this question.

Have we not by now determined that indeed this is not a pile of junk, that indeed our failure rate is sufficiently low that we can take off this coupling which interconnects to a degree the various independent channels and say that surely by now we have assured ourselves that the failure mechanism which never gives us any trouble is indeed not giving us any trouble here and that we should therefore withdraw from the situation where we compromise the independence of the various channels by the data link?

So my question is what is our experience? Haven't we by now shown that the failure rate is acceptable?

MR. KERR: I don't think that is a question. I think that is a declamation.

(Laughter.)

MR. KERR: But I accept it for that.

MR. EPLER: Well, I do have a question. Have you not by now shown that the failure rate is acceptable or have you not?

MR. SPINELL: Mr. Epler, I think I would like to ask Mr. Tom Cogburn from AP&L to address that.

MR. LIPINSKI: That is the next discussion.

MR. KERR: Are you going to discuss your experience with the data link?

MR. COGBURN: Yes, I can.

MR. KERR: Are you willing to wait or do you want an answer to that question at this point, Mr. Epler?

MR. EPLER: At any time.

MR KERR: Okay. I would suggest that you do that because I think you need to put your answer is some context rather than answering it yes or no.

(Slide.)

MR. SPINELL: Let me then refer to the safety evaluation report and the open item as it is currenty listed in Section 1.3 or Chapter 2 of the SER. The SER item embodies three items listed thusly.

Over on the right I have identified the documentation that we prepared for independent staff review with respect to these items.

In each case we have submitted a set of function description or data base documentation which we believe meets the staff requirements. I understand that the staff will talk later today about this documentation.

I can this much. We are in a stage of review with the staff and back and forth in a question and answer kind of mode at this point on that documentation. This documentation is to the same level of detail as what was submitted on the Arkansas docket and what was reviewed during that time frame.

MR. KERR: Is it your view that given time to review the information available to the staff they probably have enough information or would your experience up to now indicate that in order to complete the review you are going to have to provide additional documentation?

MR. SPINELL: Well, we may have to provide some additional documentation to show more detail on certain calculations instead of identifying results, but that is not in our opinion going to be a time-consuming process because that work is basically done at this point.

We will probably interact with the staff considerably over the next month or two to converge on this item and to help them progress and complete their review.

MR. KERR: Thank you.

MR. LIPINSKI: A question on that last item on the thermal hydraulic methods. Are you going to cover that in detail in the discussion after lunch on software changes?

MR. SPINELL: Correct.

MR. LIPINSKI: Okay.

(Slide.)

MR. SPINELL: My last slide this morning is an identification, if you will, of other relevant licensing items with respect to the software package itself, the software qualification package, and I have listed two items here.

First, the actual methodology or the framework by which we go from a conceptual stage to a fully qualified implemented stage of a particular software item that we want to correct, modify or update.

Secondly, the software testing program that is underway for San Onefre Units 2 and 3.

The software change procedure methodology which will be covered in greater detail this afternoon is embodied in a document CEN-39(A)-P listed here and its supplement. The document embodies a complete methodology from conceptual design stage through design implementation and qualification, including the test cases that are required for the test program, the test fixtures themselves and the test facility.

This document was submitted to the staff for review and it was approved for use with that single channel facility in Windsor.

MR. LIPINSKI: What was the date for Revision 2 and the supplement? Are they recent documents or are they old?

MR. SPINELL: They are not recent in the sense of a few months.

Bill, can you help me a little more on this?

MR. LIPINSKI: Well, they were issued since ANO-2 review?

MR. SPINELL: They were issued after the initial fuel load license for Arkansas.

MR. LIPINSKI: Okay.

MR. SPINELL: December of '78 I think is the date on the document supplement.

I would like to further point out with respect to this change procedure methodology that Edison has committed to the use of this approved method to implement the software changes that we will be discussing this afternoon. This document then provides the framework for the existing functional description and test program documentation which we have. In the case of the test program we will be submitting to the staff within two months.

The second point with respect to the software testing program itself, in that we are performing it in accordance with the CEN-39 as I pointed out, the results of that test program for the various data and dynamic cases in the Phase 1 and Phase 2 types of cases that we will be running in accordance with that procedure as I identify will be submitted in April '81.

In summary this this morning for my presentation I have tried to provide you with an overview of the system, a comparison of the San Onofre and Arkansas designs, the status of the field equipment and the design and licensing activities associated with that equipment.

In an overall sense we are in an advanced stage of work with respect to both the hardware and the software both in the field and at the Windsor site with respect to qualification.

MR. KERR: Does that complete your presentation?

MR. SPINELL: It does, that is correct.

MR. KERR: Are there questions?

(No response.)

MR. KERR: Can you or will someone else indicate how you have taken into account the experience with ANO 2 in any changes or corroborations of the CPC design which you are going to use on San Onofre?

MR. SPINELL: Well, Dr. Kerr, the next speaker, Mr. Tom Cogburn, will be providing you a detailed assessment of the ANO 2 experience.

MR. KERR: I understand that. What I am trying to find out is how you have used that in order to either say, hey, CPC was great the way we originally designed it or we need to make these changes.

I recognize he is going to tell me about the experience and maybe it makes more sense to answer my question after I have heard more about the experience.

MR. SPINELL: We will be covering the second half of that in the afternoon.

MR. KERR: Okay.

MR. SPINELL: We intend to give you our experience first and then to show how that experience was incorporated or is being incorporated into the cycle one.

MR. KERR: That sounds eminently logical.

Are there other questions?

(No response.)

MR. KERR: Okay. The next man up is from ANO 2, Mr. Cogburn.

MR. KENNEDY: Dr. Kerr, I would like to point out that Mr. Spinell in his presentation has effectively covered Item 5 in the agenda, the San Onofre design and test status with his slide that reviewed that test status. We will not be covering Item 5 again so there is 15 minutes we can gain.

MR. KERR: Thank you, sir.

MR. KENNEDY: Now I will turn it over to Mr. Cogburn. Mr. Cogburn is Superintendent of Plant Analysis at Arkansas Power and Light.

PRESENTATION OF TOM COGBURN

SUPERINTENDENT OF PLANT ANALYSIS

ARKANSAS POWER AND LIGHT

MR. COGBURN: Thank you, Mr. Kennedy and Dr. Kerr.

My talk today is about the operating experiences at ANO 2, particularly with respect to the core protection calculator system.

I will go into the operating experience of the plant, the operating history a little bit. I will spend a little time on the core protection calculator field start-up testing. I will discuss the problems that we have had and some of the solutions that have been effected in our plan and will end with an evaluation of the system from Arkansas Power and Light's point of view.

The slides that I have do not cover in detail all of the topics. They have boiled down a lot of detailed information and I tried to cover the topics which I felt the ACRS would be most interested in having in hard copy.

(Slide.)

First of all, a brief summary of the ANO-2 milestones. The operating license was received on July 18, 1978. We began initial fuel loading July 23rd. Following that, a post-fuel loading hot functional test period, and then initial criticality in early December.

We first reached 100 percent power in January of 1980. You will notice that there is an extended period of time from initial criticality to achieving full power. Of course, one thing that affected that was the accident at Three Mile Island which occurred in that timeframe.

Also, we had fairly significant problems with our main steam safety valves which eventually had to be replaced in total, and we had some significant failures in emergency diesel generators.

The testing program was conducted primarily -- the power phase of it was conducted primarily in the summer of 1979 and completed, largely completed in early 1980 with commercial operation on March 26th of 1980. We anticipate beginning our first refueling about a month from now.

(Slide.)

ANO-2 is rated at 15 megawatts. The first cycle design burnup is 12,500 megawatt days per metric ton, and this is equivalent to 326 effective full power days. The burnup history I have given here for reference, this is the amount of burnup accumulated in a year -- not a cumulative number, but only the amount in that year.

We were at low power and only started up in late '78, so there was very little burnup in '78. In '79 there were many equipment problems, and we were involved in low power testing through a lot of the period.

In 1980 the performance of the plant and the burnup achieved was considerably larger, and through the early part of 1981 it has been very good.

The capacity factor after achieving commercial operation in this first cycle up to the middle of this month has been 65 1/2 percent roughly.

MR. KERR: And commercial operation began at the beginning of 1980?

MR. COGBURN: Correct. It was March 26 of 1980.

MR. KERR: Thank you.

MR. COGBURN: The items that I intend to proceed with next are startup testing program, and then following that the CPC system performance during testing period and during operation during this first cycle.

(Slide.)

This slide shows really just a list of the tests that were performed. Basically, the testing program regarding the core detection calculators went very well. There were no required hardware or required software changes that resulted from the test program. All of the testing was completed satisfactorily. There were minor modifications to addressable constants, many of which were expected, some of which were not expected but were easily accommodated.

Prior to criticality a test we called CEA exercise test was conducted. This was basically just a movement of the control rods in various operating configurations, both normal and off-normal, and verification of the proper indication of rod position with the CEACs and CPC system and also the control system and plant processor computer.

We also verified the correct calculation and look-up within the CEACs and CPCs based upon deviation or overlap, rod overlap, exercise limits, etcetera. There were no anomalous findings during that test.

We also conducted a response time test in the core production calculator inputs. These response time tests were primarily from single input through trip generation-type test. The CEA response time was conducted by a rod drop at subcritical condition with simulated inputs for -- written into the computer for other signals.

The reactor coolant pump speed sensor and response time was done by a two-pump trip under similar conditions. The CEA position in the reactor coolant pump were actual plant trips. A rod was dropped; pumps were tripped. The other parameters were by signal injection, ramp, or in most cases there were step changes, and then the predicted response was done previously.

We had in the measured sensor response time to the time it took from signal injection to CE and breakers open.

MR. LIPINSKI: Substituting for the sensor input?

MR. COGBURN: Correct.

During the power ascension phase we conducted several tests related to the core production calculator system. One test referred to is the CPC verification test. We have really three different parts.

The first, at the power level shown here, involved a comparison of field-measured inputs and outputs for DNBR and local power density from the CPC system, and these were compared off-line after the fact by inputting those same inputs into the Fortran version back at Windsor. And the Fortran version statistically varied the inputs and outputs in the expected range of this, which we used to compare and verify that the CPCs were proper calculating in the field as they should.

Also, at the request of the NRC staff a test was performed at various power levels to evaluate the noise and core calculator protection system. These tests involved recording of process signals, taking the data bank to Windsor, using the hardware at Windsor to compare a noise-free signal to one with process noise, and verify that process noise always made the resulting DNBR and LPD conservative.

Also, at the request of the staff we conducted an electromagnetic interference survey. This was done at one power level in the control room, in the core protection calculator room which we had for calculators. Surveys were done, and the signals that were measured were compared to minimum susceptibility for interference limits that had been established previously, and the signals measured were considerably below the thresholds.

MR. LIPINSKI: Could we go back to number one, the CPC versus Fortran? Did you record all the input parameters to the CPC as well as their outputs?

MR. COGBURN: Yes, we did.

MR. LIPINSKI: And this is how the comparison was generated?

MR. COGBURN: We observed the CPCs for a period of time -- several minutes -- and determined the minimum and maximum value for each and every parameter and also observed the minimum and maximum output per calculated result, the DNBR.

MR. LIPINSKI: Did you do any rod drops or any initiating transients, or is this just a static comparison?

MR. COGBURN: This is a static comparison.

MR. LIPINSKI: Did you do any effort on dynamic performance?

MR. COGBURN: Not in the field, no. The C-SEC verification which is -- some tests were conducted regarding the CE code, C-SEC, for transient analysis, and there was a little data generated at that time but not specifically for that purpose.

MR. LIPINSKI: So this system is installed, and all you know is that it has steady performance, but you have no verification of dynamic performance?

MR. COGBURN: The dynamic performance is evaluated by off-line testing of the software compared to many cases that are generated by the design codes for design of the plant. This will be described in the startup -- excuse me -- software change procedure discussion later.

MR. LIPINSKI: I'm aware of the procedures testing it off-line, but it seems like one or two dynamic tests would have been beneficial.

MR. GILL: Excuse me. You did run the rod drop in --

MR. COGBURN: Yes, that's correct. We did. Those tests included evaluation. There are a couple of tests that I did not include here -- a loss of flow test from 80 percent power, a tripping of all reactor coolant pumps, which part of that test -- part of the purpose of that test, one of the C-SEC verifications of the test was to evaluate the CPC performance.

MR. LIPINSKI: Now, were the input parameters recorded in the CPCs as well as the outputs in the course of the test?

MR. COGBURN: Some of them were, the ones that could be recorded from the analog signals that exist. The data links to the plant computer cannot access or do not access at that frequency. Maximum time was ten seconds from scan.

MR. LIPINSKI: The system works under dynamic conditions.

MR. COGBURN: We measured the time to trip for that condition. We also did a couple of rod drop tests which were performed where we recorded system parameters, CEA position, etcetera, and also measured the trip time.

I believe the important inputs to the analysis were recorded, but not all of the inputs could be recorded.

MR. LIPINSKI: Okay. Thank you.

MR. COGBURN: I'll go very quickly through the rest of these tests. The flow rate measurement, the calibration that Bill Gill mentioned earlier, we called it the RCS calorimetric flow rate measurement. This test was performed to verify adequate reactor system flow and to adjust the CPCs to the measured flow, minus some drift allowance.

CEA shadowing factor was performed. The measurement was performed to compare the ex-core detector response observed to CEA insertions with those that were installed or inspected in the CPC system.

Temperature decalibration --

MR. KERR: Excuse me. Would you say a little bit more about C?

MR. COGBURN: How it was performed?

MR. KERR: Or what it -- it is referred to as a shadowing factor measurement, and I just wondered what one measures as a shadowing factor.

MR. COGBURN: Control rods, when inserted in the core, especially peripheral rods, have a significant effect on the ex-core detector response because of their shadowing or shielding effect.

MR. KERR: That I understand, but what is it you measure?

MR. COGBURN: We measure in this case the neutron detector response with CEAs inserted and not inserted, and compare those to the calorimetric power level and adjust the signal response or verify the signal response of the neutron detectors is adequately compensated. We also use in-core detector signals for power distribution from the core.

MR. KERR: I guess I can't tell then whether C. was an effort to verify previous calculations or was in effect a calibration procedure.

MR. COGBURN: It was both. In effect, the purpose was to either verify that existing correction CEA shadowing factors were adequate within the acceptable margins or to verify that by changing addressable constants, they became acceptable.

In this particular test we did require additional uncertainties to be added in the addressable constants to cover a small amount of difference between the shape -- excuse me -- the shadowing factors built into the CPCs and those measured.

There were no addressable constants that explicitly included to adjust CEA shadowing factors in the original design.

MR. KERR: In an RCS calorimetric flow measurement what does one measure, flow rate or power or --

MR. COGBURN: We assume the biggest unknown in the primary heat balance is the reactor system coolant flow, so basically we do a heat balance across the steam generator, the primary calorimetric as compared to the secondary calorimetric, assuming all of the inputs or knowns, with the exception of reactor system coolant flow rate, and then those two equations are solved for the known system flow rate.

MR. KERR: So you assume that you can measure accurately the heat rate in the secondary heat output?

MR. COGBURN: Yes, that's true. Prior to this point we had done --

MR. KERR: No. I want to understand what you did here. You assume a secondary heat balance is a known.

MR. COGBURN: The industry practice, which I'm sure you're well aware of --

MR. KERR: No. I'm not well aware of industry practice.

MR. COGBURN: There is --

MR. KERR: Believe it or not, there is occasionally one of these documents that I don't read.

(Laughter.)

But assuming that the secondary heat balance is known --

MR. COGBURN: Yes.

MR. KERR: You then do a primary heat balance with the flow as an unknown, and you calculate the flow on that basis, is that what it amounts to?

MR. COGBURN: Yes, sir.

MR. KERR: Thank you.

MR. LIPINSKI: Your flow in the primary system is by delta P on elbows, is that correct?

MR. COGBURN: We have pump speed.

MR. LIPINSKI: No, forget about the pump speed on the CPCs, but you did have delta P measurements across the elbows, I believe, do you not?

MR. COGBURN: Across the pumps.

MR. LIPINSKI: Not across the elbows at any point for a pressure dump? No? Okay. That's a Westinghouse plant then.

MR. KERR: And it is industry practice to assume that this secondary heat balance can be made within two percent or something like that?

MR. COGBURN: That's correct.

MR. KERR: Do you believe that?

MR. COGBURN: Yes, I do. If it's properly -- if the instrumentation is properly surveilled and maintained as it should be. The CPC assumes the accuracy of the RCS calorimetric load to be 3 1/2 percent, I believe, and that uncertainty is built into the CPC system.

MR. LIPINSKI: What's the accuracy then on your total thermal power?

MR. COGBURN: Two percent.

Shall I continue?

MR. KERR: Please.

MR. COGBURN: I believe the next test that I have not discussed is the temperature decalibration measurement. This is also measurement of the effect of temperature changes, cold leg temperature changes upon the response of the neutron detectors, the ex-core neutron detectors.

MR. KERR: Can you tell me what a decalibration is?

MR. COGBURN: The amount of change or inaccuracy that is induced by changes in the coolant temperature unless -- in the standard PWR design prior to ANC-2, I believe all plants such as our Unit 1 do not compensate for this directly. It requires a manual calibration. The effect, of course, is cold leg temperature decreasing, higher moderator density, less neutron flux reaching the ex-core detectors, causing a decalibration.

For the same power if you drop cold leg temperature, the response of the neutron detectors becomes decalibrated in a non-conservative direction.

MR. KERR: Would this mean the same thing if it were called temperature calibration measurement?

MR. COGBURN: It wouldn't to me. It might to someone.

MR. KERR: Okay. Because it would seem to me from what you've said, you are calibrating the system to take account of temperature effects.

MR. COGBURN: That's correct. The CPC system does this automatically on-line. The radial peaking factor verification involves setting up different control rod conditions in critical geometries at steady power level and measuring with the in-core detectors the radial power distribution, calibrating the maximum radial peaking factors using in-core detectors and in-core analysis codes, and then comparing these calculated radial peaks to those in the CPC look-up tables, and verifying that the measured values were more conservative or smaller values than the CPCs assume given rod configuration.

This was in fact the case. I think the magnitude of conservatism was varied, from 4 to 10 percent roughly depending on which CEA banks were inserted.

MR. KERR: These were compared with radial peaking factors calculated for 50 percent power?

MR. COGBURN: Yes. The radial peaking factors are actually not power level dependent.

MR. KERR: How do you know?

MR. COGBURN: I would see if someone from CE could answer that for me.

MR. KERR: I thought that's the reason one measured them, because one was trying to verify the fact that calculations are valid.

MR. COGBURN: That is not really the purpose of this test, but we also verified core power distribution measurements. I did not detail all of the procedures that we ran by any means, but I just picked the ones that were specifically run for CPCs. But there were several other core power distribution verifications to go back to design comments. This was simply a checkpoint really on the CPCs.

Mr. Gill.

MR. GILL: Bill Gill from Combustion Engineering. Let me have one item on the radial peak power dependency. The analytical calculations that are now predicted, the power peaks to be power dependent, but that is of little importance when you have the ability to measure.

CE does have a core follow program on many of our operating reactors where we get monthly snapshots of in-core detector ratings at various power levels, and these snapshots are continuously used to validate the design codes, and that's the basis for this statement.

MR. COGBURN: The other CPC specific test was actually conducted at 20 percent and 50 percent of power, as opposed to what I have written here. The shape annealing matrix test involves establishing or setting up an axial xenon oscillation at a stable power level. This is done by achieving criticality with the lead bank control rods inserted in the midpoint of the core, operating for several hours to achieve near-equilibrium xenon conditions, then withdrawing them rapidly.

This -- at 20 percent power the oscillation that we induced that way dampened rather quickly. At 50 percent power it lasted for well over 60 hours, which was the goal. And the reason for doing it that way was to establish a large variety of different axial shapes.

During the test we measured and recorded the ex-core detector signals, using the CPC-to-plant computer data links and various other inputs to the CPC in that manner, and recorded the power distributions that result basically -- the in-core detector measured power distributions recorded concurrently.

Then the shape annealing matrix is a square fit for the three detectors in each channel, which compares the in-core detector, three segments of the core -- or three segments of the core, top, middle, and bottom, based on in-cores to top, middle, bottom signals from the ex-cores.

The boundary condition is just measuring the reflector savings point or the point where the flux goes to zero from in-core detectors.

The objective was to calculate a matrix that would be representative of the -- of many different shapes and would be able to be used to synthesize from the three ex-core detector signals and the boundary points from those five points an axial shape -- an axial power distribution for the core.

So we determined the shape annealing matrix and put that into the CPC system and made some minor adjustments to the boundary condition by way of additional uncertainty factors through addressable constants.

MR. LIPINSKI: This was done by analysis prior to your going into operation. How close did your measurements compare to the analysis that had been done previously?

MR. COGBURN: I don't think there was ever any expectation that they would be very close, and they were, in my opinion, not that close.

It's very difficult to predict the ex-core detector response, of course, because of the complicated geometry around the reactor vessel. The concrete structural members and so on are not really possible to model. But the response of the upper and lower chambers was better than predicted.

So with the predicted shape annealing matrix or the initial shape annealing matrix, for a co-sine-shaped distribution, we actually saw a somewhat saddle-shaped distribution, a double hump. Because of this, we implemented the shape annealing matrix at 20 percent power, and we had only planned to run and implement one at 50 percent power.

And then we modified it by the results at 50 percent power, because they would be expected to be a little bit better, because the signals are larger at 50 percent.

MR. LIPINSKI: Could you refresh my memory. Were you using a fit as part of the shape annealing matrix?

MR. COGBURN: Yes. Maybe Howard or Bill --

MR. GILL: The answer is yes. We could elaborate on it if you would like.

MR. LIPINSKI: I would like a better discussion, because when you are doing the development of this system it was based on being able to make measurements with a certain accuracy on these ex-core detectors. Now you've got the experimental data. Were you surprised or not?

MR. GILL: I think the answer is no, we were not surprised. If you look at the fitting technique, it is a matrix and it is a series of numbers, a three by three matrix. A very small change in that matrix can have a large impact on the power distribution.

I think our ability to predict was good. We knew that one of the most vital or critical measurements in terms of CPC callibration was the determination of that matrix.

But, as Tom had mentioned, our ability to calculate the transport of neutrons from the peripheral bundles out to the ex-core detectors is one we did not have a high degree of confidence in. It is a complex phenomenon where it is actually faster with neutrons getting to the detectors being slowed down, not only through the water in the vessel, but also through the concrete, with a high degree of scattering.

So we were aware that we had to make measurements and that those measurements would not really be a check or a validation of matrix, but would be a determination.

MR. LIPINSKI: Having measured this double hump rather than the uniform distribution, are you now able to explain the double hump by analysis?

MR. COGBURN: I don't -- well, refer that to Bill again, or Howard.

MR. GILL: We could have our physics people try to explain that. It would probably take a half hour or more. I can't explain it.

MR. LIPINSKI: I don't know that it's necessary at this time.

MR. KERR: Well, the question simply was, I think, whether you were able to explain it. You didn't ask for an explanation.

MR. COGBURN: And the answer is yes, I believe.

MR. KERR: The answer seems to be being formulated at this point.

(Laughter.)

MR. GILL: I think we have a consensus vote. We understand why it happened and we understand the phenomenon which resulted in the double hump.

MR. KERR: So the answer is, I think, that qualitatively it can be explained, but it has not yet been explained quantitatively; is that fair?

MR. GILL: I think it's been explained both qualitatively and quantitatively. It's a repeatable phenomenon where we understand how we calculate the matrix that was there and we understand how the ex-cores were processed and why we came up with a double hump.

We know what we did to fix it, and there is no surprises or unknowns in the scenario, in the power distribution.

MR. LIPINSKI: Had you approached the problem from the design standpoint in the forward direction, could you generate a double hump?

MR. GILL: There's always a matrix I can find that would give you a double hump, given the ex-core readings.

MR. LIPINSKI: That's not the question. Given three detectors stacked one on top of another, with the shape of the flux within the core, would you be able to predict that those ex-core detectors would measure a double hump?

MR. KERR: I guess I'm not quite sure what you mean by the question, because are you asking, given the state of knowledge before they made this measurement or the present state of knowledge? Clearly, with the existing information, one could predict the double hump. Either you or I could do it if we knew it existed.

MR. LIPINSKI: That's not the question, because they have a technique --

MR. KERR: Are you asking whether they could predict it before they had the existing information or whether they could predict it now?

MR. LIPINSKI: Whether they could predict it now, knowing that it's a phenomenon that does take place.

MR. KERR: With five good Combustion engineers, they could do it. There's just no question about it.

MR. LIPINSKI: Well, what's bothering me is whether they have even looked at their analysis techniques to explain why it has taken place. I know of the fact that it has taken place. Fudge factors have been put into the matrix to make it match what they have measured.

MR. COGBURN: Well, I think in a sense it was expected all along, as discussed with the NRC staff during review, I know. I'm not sure of the ACRS. It was expected that we would not predict the shape exactly right.

MR. LIPINSKI: But in all of the prior review there was no anticipation of a double hump.

MR. COGBURN: I don't know about that. You expect to see double humps.

MR. GILL: Let me turn this over to Howard Neuschaeffer, who actually analyzed the data from the plant. He can give a summary that might help you analyze your question.

MR. KERR: Can he do it in less than five minutes?

MR. GILL: Let me check.

Yes.

MR. NEUSHAEFFER: I think there is first a minor degree of confusion here in that the double hump distribution was not a real measure distribution that was double humped. The power distribution in the core at the time of measurement was a co-sine distribution, so that we were expecting to have a co-sine.

The preliminary shape annealing matrix that we had installed was based on prior calculations, which are a fairly difficult calculation to perform in terms, as mentioned by Mr. Cogburn, of you have got a very diffused degree of scattering out there in the cavity.

As you get from the core and the vessel and bounce around the structure, your neutrons are doing all kinds of weird things. So you make estimates of this, using some fairly difficult techniques. And it's a calculation that tends to be uncomfortable. You're uncomfortable with relying on the results too much.

So we went in and developed this test procedure where the calculation of the matrix was verified experimentally. Now, what would have been nice, were it possible -- and it does not seem to be possible, with the state of the data we were able to measure -- is if we could go in and predict the scattering of core neutrons or measure the way the core neutrons will scatter from various parts of the core to the detectors in enough detail that we could go back and precalculate a good shape annealing matrix and not have to do this measurement again.

What we did instead is, we get the matrix itself, which is a three by three, nine data items, rather than a detail of about 20 by 3 or some 60 data items that you would need to try and do the prediction of the ex-core, of the shape annealing matrix very accurately.

So I think the situation is that we know what has happened. We understand the basic phenomenon that we -- our calculation of the neutron scattering effects was not as good as we would like it to be, but there does not seem to be at this point a way of improving that in a calculationally feasible way.

In principal, you could run thousands of hours of computer calculations and perhaps improve it. What you are getting instead is a measurement technique that will allow you to account for the fact that this is a difficult calculation to do and that it is in effect a callibration procedure of this particular component of the CPC's to the real situation.

MR. LIPINSKI: May I summarize what I thought I just heard? Given experimental data, you still say you cannot take your analytical results and modify them to predict what you measured experimentally.

MR. NEUSHAEFFER: No, I didn't quite say that. I said I cannot take my measurement data and use it to predict a shape annealing matrix which will be as good as the measured shape annealing matrix. I can measure better than I can predict this phenomenon, because the measurement does not have enough detail in the axial sense to allow me to calculate better.

MR. LIPINSKI: Maybe we're saying the same thing. Let me say it again. Given a co-sine flux distribution in the core and the transport of neutrons from the various regions in the core to the three detectors, can you now make a better prediction as to what each detectors sees, integrated over the total length of that core?

MR. NEUSHAEFFER: In a sense better, but not good enough to alleviate the need for this measurement.

MR. LIPINSKI: No. Given the measurement, can you then adjust your calculational techniques?

Are you trying to do it? That's the next question. I suspect that you may not have. All you've done is put the fudge factors in.

MR. GILL: There's nothing we see in a power plant that we don't go back and try to understand our analytical methods. So the answer is we've gone back and modified our analytical methods to the extent practicable. It is not sufficient to replace the measurement.

MR. KERR: Mr. Gill, I'd be careful if I were you, because I believe that with today's state of the art, if you want to spend the necessary money, you could calculate this. I think it would be foolish to do it, but it's within the state of the art.

It seems to me the important issue here is whether you can use this particular matrix for a different power shape in the core. My guess is you cannot, because you have arrived at the matrix on the basis of a co-sine power shape, and if you get something in the core that is different from the co-sine power shape, it seems to me you have some difficulty demonstrating that you could use this matrix.

Now, perhaps you have arrived at several different matrices, each of which is appropriate to a different power shape. Or perhaps you always have a co-sine power shape, which I doubt.

MR. COGBURN: One of the purposes of the surveillance, the core follow program, we call it, is to verify that the CPC axial shape in synthesis is adequately reflected throughout the cycle. And we have observed that the shape annealing matrix has been adequate for this first cycle. We will determine a new one.

MR. KERR: But that may simply mean you have the power shape through the first cycle that is about the same as the power shape you used to derive the matrix. And it seems to me the question is whether you could use it if you have a rather different power shape.

MR. NEUSHAEFFER: The answer to that question is you can use it for a range of power shapes, the reason being that the measurement of the matrix itself covered a wide range of power shapes.

The oscillation that Mr. Cogburn mentioned included ASI ranges from, I believe it was, plus .2 to minus .2, approximately, which is a fair range of shape at beginning of cycle. So that you have covered both top and bottom peak and center peak shapes in the measurement.

The matrix is thus kind of a weighted average matrix, which will cover that range of shapes. If you get later in cycle and your power shapes tend to flatten in the center and go saddle, calculations have indicated that you will become more conservative in your estimate of both linear heat rate and DNB, since your beginning of cycle shape measurement will have left you with a shape annealing matrix that tends to make you appear more highly peaked.

It's a higher axial peaking factor than your axial shape would have. So you tend to build in with lifetime a little bit of extra conservative calculation, because the CPC will think it has a somewhat more peaky shape than it really does.

So we have considered that. And we have also, in our uncertainty assessments, looked at a much wider range of shapes out to the full range of what CPC has been qualified for. And the uncertainty values themselves include an allowance for the fact that you can possibly get shapes which are wider than the range of shapes that were actually used in the measurement.

MR. LIPINSKI: Has the topical report been written on the experimental work in comparison to the original analysis?

MR. COGBURN: The ANO-2 startup report documents the comparison of this information. I have a copy with me if you would care to look at it, a copy of that portion.

MR. LIPINSKI: Mr. Chairman, when we reviewed this system initially there were these concerns with respect to the shape annealing matrix. And from the discussion that is proceeding now, you now have the feedback from experimental information back to the original analysis.

And I have not seen the report referred to, but I think there is a question here in terms of performance of the system and how these constants are being handled in this shape annealing matrix. I wouldn't propose that we go into it in detail at this time.

MR. KERR: Okay. You might think some about what you would propose.

Please continue.

MR. COGBURN: Thank you.

In conclusion, regarding the startup test program, it was our conclusion that the testing was accomplished accurately and some minor adjustments were necessary, but all within the capability built in the core protection calculator system.

We did identify some desirable features in-- to make changes in the area in software, and these are planned and they will be described later on in the afternoon.

The next area I intend to cover is the experience, or really, the problems that we have had with the core protection calculator system. The initial performance of the calculators has resulted in a number of failures and trips. I will go into those in detail.

The kind of problems that we have had are basically -- I haven't put a slide up here yet -- room and cabinet cooling, AC power supply inverter problems, connector problems, insufficient diagnostics. And there were a couple of algorithm oversights. And I will discuss how they occurred and what we do about them.

First of all, the CPC's have initiated a number of plant trips -- reactor trips, a total of 28 to date, including one that occurred about a week ago. The numbers and when they occurred, I have broken down on this table.

Of these trips, I'm going to use the terms "valid trips" and "non-valid trips." By valid trips I mean the CPC's were responding in their trip to some plant event, design basis event which occurred. And by non-valid trips I mean spurious trips or trips that occurred because of a hardware failure, because of an error, a human error, or because of a spurious signal of some sort.

(Slide.)

The valid trips on this list are nine: four of them in '79, four in 1980, and one in 1981. The rest are, quote, "non-valid trips," and I will go into a slide that breaks this down a little further in a moment.

I would like to point out here that the CPC's and all of their failure mechanisms that we have observed have always failed safe.

MR. KERR: Mr. Cogburn, do you know, during this period during which 28 trips were CPC-initiated, how many total trips you experienced? Not exactly, but 2 or 20 or 50?

MR. COGBURN: 70.

MR. KERR: 70?

MR. COGBURN: Many of these trips occurred at very low power levels, one percent or less.

MR. KERR: Does 70 include these 28?

MR. COGBURN: Total.

MR. KERR: Thank you.

MR. COGBURN: I can give you an exact number.

MR. KERR: That's close enough.

MR. COGBURN: I would like to point out that the majority of these trips occurred prior to commercial operation in the early part of the cycle. If you go back to the second slide, very little burnup had occurred at that time.

Since commercial operation, the number has been eight.

MR. LIPINSKI: For the date, you are using March 26th, 1980 as the dividing line?

MR. COGBURN: Yes. I believe 74 full power days before commercial was the number I had there -- no, excuse me -- yeah, 74, approximately 220 power days since commercial.

I have plotted a curve for the frequency of trips and the amount of core burnup that has been achieved beween CPC trips and just non-valid trips.

(Slide.)

Because I think that is probably of concern or interest, versus time. I just averaged the numbers that occurred over time, and I tried to account for the operating down time by factoring in the burnup that occurred in this time period.

So I would like to point out here that the frequency of trips or the time between trips is increasing -- has been increasing all along, particularly since the early problems were resolved. We are going to discuss today a couple of software modifications that were made.

MR. KERR: I have a suggestion. I think that curve would look better if you rotated it 90 degrees, but that's incidental.

MR. COGBURN: That way?

(Laughter.)

MR. COGBURN: Well, I like it this way.

MR. KERR: Okay.

(Laughter.)

MR. COGBURN: But I'm sure I respect your opinion.

The two software modifications that I was referring to did occur approximately here and here in time, and I think they had something to do with the improved performance.

(Slide.)

MR. LIPINSKI: Let me make sure I understand. Each point on that curve was a trip? No?

MR. COGBURN: Actually, that is -- I realize this is kind of confusing. I had a hard time figuring out how to present this. But what it is is each point is not a trip. It may be several trips.

MR. LIPINSKI: It says "between trips," though.

MR. KERR: It's an average over a period.

MR. COGBURN: It's an average over a period that accounts for the operating time in the plant. It normalizes it.

MR. LIPINSKI: You could have put it in the right form. Since this is integrated time, you could have put it in the right.

MR. COGBURN: That's true. It might have been better.

MR. LIPINSKI: You didn't know that you got all this good advice from the ACRS Subcommittee, probably.

(Laughter.)

MR. COGBURN: I'm pleased to have it.

(Laughter.)

MR. COGBURN: I would like to point out, as an excuse for maybe the poor quality, there was very little time.

MR. KERR: It's an excellent quality slide.

(Laughter.)

MR. COGBURN: Thank you. I drew it myself.

(Slide.)

I said that I would try to break down the cause of the trips and then describe the reasons for them, and I will attempt to do that. Of the 28 trips, we have attributed 12 of those to hardware failures. All of those hardware failures were related to the CEA position input and are a direct result of the one out of two design with the core element assembly calculators -- control element and assembly calculators.

Seven of those 12 trips were caused by an intermittent hardware failure. One specific hardware failure that we had a lot of trouble defining, it wasn't until after some additional diagnostics had been added and a software change, that we were able to determine the failure and repair it, and that was done in June of 1980.

These all occurred on CEA No. 2.

MR. KERR: What sort of hardware was it that was intermittenting?

MR. COGBURN: Cable, an open cable. It was a section -- well, connector. We narrowed it down to a piece of cable with connectors on it about yea-long and replaced that.

The other five were independent similar problems, but independent of that one. What it was was a single CEA position, rod number 67, position indication to CEA number 2, was intermittently going to zero. So it looked like a dropped rod as far as that CEA. That's what we put.

It generated a large penalty factor. The CPC is solid and dropped all four channels.

MR. LIPINSKI: I missed the first part of your statement. Did the CEA's actually drop or not?

MR. COGBURN: No, it was a spurious signal, a hardware failure. The CEA's did not actually drop. There are CEA drops in here and I will get to them next.

MR. LIPINSKI: Well, that's a mislabel.

MR. COGBURN: No, that's B. That's the second item.

One other thing I would like to say while I am still on the hardware failures is, I said we improved -- this situation was improved by software. And Mr. Rozek of

Combustion will describe that in more detail.

But the one feature I would like to describe out of that is we added a feature to try to discriminate out failures of CEA position. That was done by a rate of change of CEA position. If the rod was indicated to fall faster than it could physically fall, then that failure is now not considered valid and it causes that input to be marked as failed and that calculator is not used. The other one is relied on.

MR. LIPINSKI: I'm going to make a note. This is another change that was not in the original review.

MR. DITTO: I'd like to comment here on your statement earlier that all of the failures were safe failures.

MR. COGBURN: Well, the reactor protection occurred.

MR. DITTO: Now, the reason this thing was detected was because you had one failure which went to the CEA calculator, and then it went from there to all four channels. Had it been a safe failure you might never have known it existed -- I mean unsafe failure. Excuse me.

So your statement that all of the failures, all of them you saw were safe failures -- but then there could have been a dozen or a hundred, even, unsafe intermittent failures that you didn't see because you weren't testing or you didn't have an accident. So be a little careful.

MR. COGBURN: I cannot refute what you are saying, but I completely believe that --

MR. DITTO: I believe it. But then it's not obvious from the data you have.

MR. KERR: I thought what he said was all of the failures we observed were safe failures, and I don't think --

MR. COGBURN: If there were any that occurred that were not observed, I can't say anything about them.

(Laughter.)

MR. DITTO: It's almost obvious, though, that all you observed will be the safe ones.

MR. COGBURN: No, I don't think so. There are other ways of detecting failures that may not result in channel trips issuing. And what I'm saying is that all failures that occurred of instrument nature or processing nature or timing or anything have always resulted in CPC trips.

MR. KERR: There's a design criterion and it says all failures have to be safe failures.

MR. DITTO: It's obvious.

MR. LIPINSKI: Let me summarize what I think I just heard. You have hardware failures indicating spurious rod drops, and in order to inject hardware failures you have now modified the software.

MR. COGBURN: Yes, that is correct. We have done other things also.

MR. LIPINSKI: Rather than fixing the hardware failures, you now have modified software that's going to look the other way and say this is a hardware failure, it's not a legitimate failure.

MR. COGBURN: We have also tried to correct the hardware problems as well, because the problems have been typical in my experience of instrumentation systems. When they are started up, connector problems are common with new systems, and you will always have such. You cannot eliminate them.

But we have tried to eliminate open signals, shorts, this kind of thing, through testing and through replacement. And it might be a good time to point out that AP&L's maintenance practice or philosophy of maintenance practice is to not replace components until we know the class of failure.

Even though we have a general area pinned down as to the failures in here, we do not go replace in a shotgun fashion several components, saying, well, somewhere in here we replaced that. We might have had better plant availability if we had done that, but our philosophy has not been to do that.

It has been to try to narrow down the problems and eliminate the startup problems and new system problems. Because our experience has shown us in the long run that it pays.

MR. LIPINSKI: What disturbs me is your philosophy of not fixing a cause, but going further downstream.

MR. COGBURN: We are doing both, sir.

MR. LIPINSKI: There are other ways to fix a hardware problem. You have a variety of things at your disposal.

MR. COGBURN: This is something we are evaluating right now. That is a major change, though, and it requires a serious evaluation to go in and change the miles of wiring involved in the system.

MR. KERR: When you get this spurious signal that might be caused by hardware failure, does the total system ignore that or does it record it but just not trip the reactor?

MR. COGBURN: It records it but does not trip the reactor. And it also causes a failure indication on the channel affected as well.

MR. LIPINSKI: But the recording is via the connection through the plant computer?

MR. COGBURN: No, sir. The recording is a software diagnostic that was added.

MR. LIPINSKI: So that it comes off on an on-line typewriter?

MR. COGBURN: No, it is recorded in the core memory. The parameters are recorded in the core memory. And then you must hook up a teletype in an off-line mode to dump this information out, or some of it is just playable through the operator's module.

MR. LIPINSKI: How often do you dump to find out that you've got misbehaving rods?

MR. COGBURN: Any time that we have an indication of a misbehaving rod.

MR. LIPINSKI: But these contacts are not going to be displayed to you.

MR. COGBURN: No, there is a flag set on the out module to tell you that it occurred, and we examine that log once a shift. And if there is a set, a value set, then we dump that automatically or by administrative controls.

MR. LIPINSKI: There weren't too many display lights on that console. Which particular one comes up?

MR. COGBURN: There is a point ID. There is a CEA fail light that comes on. But that may not stay in if the signal clears itself, which is commonly the problem that I am talking about here.

But there is also a flag set or an addressable point ID that we examine once a shift, the operators examine and see if it is set in each of the six computers. And then if it is set, we get the report out.

Also, the number of failures is logged in addressable values, not changeable values but addressable values that you can examine and see when they occurred, which sensor was affected and which direction the failure occurred in.

MR. LIPINSKI: If I have a spurious indication of a dropped rod, is there an immediate indication on the console?

MR. COGBURN: Yes.

MR. LIPINSKI: What light comes up?

MR. COGBURN: The CEAC failure.

MR. GILL: CEA failure or sensor failure, depending on where the failure occurs. It's also an audible annunciator.

MR. KERR: Any other questions, Walt?

MR. LIPINSKI: No.

MR. KERR: Please continue, Mr. Cogburn.

MR. COGBURN: I defined "valid trips" earlier as those trips that should have occurred based on the design of the system, based on a respo se to an operating event. Reactor protection we call that here.

There have been nine such trips. Eight of those were due to actual dropped control rods. One was an axial shape out of range trip that occurred at low powers following a startup after a trip, where we had a significant amount of xenon in the core and back where we were still learning how to control the xenon in the core.

The operators let the axial shape get out of range and the calculators tripped.

There's a term used here called algorithm design error. I believe "oversight" would be a better word than "error." But it is in fact an error.

There were six plant trips that occurred because of this. Five of the six were of the same nature exactly, and that was corrected by the first software modification. It was not just improved, it was corrected.

The problem was that on re-initialization of a CEA calculator, the calculator used a worst case penalty factor and had a certain probability of coming up live with that value and before it actually calculated an actual penalty factor. And so following periodic tests, it would also occur following a power fill restart or something like that.

Any kind of re-initialization of the calculator, there was a certain probability, I think estimated around 10 percent probability, that that CEAC would generate this large penalty factor, which all four CPC's would use as a penalty factor and would cause a DNBR trip.

MR. EPLER: I have a question. If I understand you correctly, the valid trips, the nine valid trips, one of those resulted from a dropped rod -- I mean, eight of them from a dropped rod. It would appear to me that your control system could have circumvented that trip and kept you on line if you had worked at it.

MR. COGBURN: Well, I think what this page points out, if you would eliminate the one out of two problems with CEA position input in some way -- I don't know what the answer is -- you would find that this 28 trips would go to two trips only. And none of them was --

MR. EPLER: The thing is really related to rod position indication failures.

MR. COGBURN: Either that or rod drops.

MR. EPLER: I would ask you if your plant computer has any connection with that at all.

MR. COGBURN: Any connection with what? Excuse me? With what?

MR. KERR: Do you understand? If the on-line computer data link would have helped this situation any, I think. Isn't that the question?

MR. EPLER: I'd like to see us get rid of that thing, but I wouldn't want to get rid of it if it has a function. But I don't see any function.

MR. COGBURN: Well, I hope to describe to you what the function is. But I hadn't got to that point yet.

MR. EPLER: Okay. I'm still looking.

MR. COGBURN: I don't perceive a connection in this particular problem with the data link.

MR. KERR: But you felt good knowing it was there, didn't you?

MR. COGBURN: Yes.

MR. KERR: See.

(Laughter.)

MR. DITTO: Did you say you could eliminate all but two of these if you didn't have but one out of two CEA arrangements?

MR. COGBURN: I did say that. I'm sorry. I'm glad you corrected me. I should have said we would have had only two if CEA were not an input to the protection system. One out of two would have eliminated all of these hardware problems.

MR. DITTO: But not the 8, because you actually dropped the CEA and both systems saw it.

MR. COGBURN: I have a comment in my statement here that the probability of plant trip was reduced again. This is different than the other one here, because the system that was initially -- this is going to be described in much more detail, but basically we had rod drops that occurred at one percent power, and they resulted in plant trips. The penalty factors were highly conservative. This was a result of, in my opinion, of having to freeze the software at such an early stage before we could refine it; but I'm not taking that as an excuse, just a fact of the way things occurred.

We did make modification -- Mod 2-B it's going to be referred to later -- which reduces the magnitude of some of the penalty factors. It becomes more position specific penalty factors rather than just a case number; so those low power rod drops should no longer cause plant trips.

There were two rod drops that occurred at full power, and they undoubtedly would also still cause plant trips, and they should for reactor protection -- fuel protection.

MR. LIPINSKI: How are the CPC channels powered? Do they have individual DC supplies?

MR. COGBURN: They are powered from AC inverters which are backed up by batteries.

MR. LIPINSKI: Now, what happens if one is turned off and it is reinitialized?

MR. COGBURN: You would have a power fail restart and the channel would trip, a channel would trip. If a CEAC were to be powered down, the way it's designed, the failed bit would be sent. The CPCs would then acknowledge the failure and say that guy is no good, I won't use it.

The technical specifications then have a requirement that we follow up on in that event, so power failure should not cause a plant trip; a single channel failure should not cause a plant trip.

The category called algorithm design areas, we covered one of them; that was the CEAC initialization problem. The other one was discovered at very low power, down around five percent power, where the software switches over from a fixed axial shape because of the low signals on the ex-core detectors to a measured axial shape, and then making that transition, the extrapolation or the -- what's the word I'm looking for -- the Update Program saw that change as going -- there was no dead band provided, so that when you go across that boundary, it would switch back and forth between a fixed shape that was very conservative to a measured shape which was not adverse. So that in going from the good measured shape to the adverse fixed shape, it would look like a rapid rate of change, and we would get a DNBR trip.

This was corrected by software modification by providing a dead band and also by providing a less conservative fixed axial shape at low power.

Mr. Rozek will describe that in more detail this afternoon.

There was also one trip which I call technician error. I believe I should have called it procedural error. It involved one CEAC in the in-op mode and the technician going to test on the other one, which made them both look failed. When the CPCs see that, they will trip. We corrected that by a procedure change, and it has not happened again.

MR. KERR: Mr. Cogburn, I need some advice from you. Our schedule shows that we're going to stop for lunch at some point. What is a good point from your point of view? Is it better to stop now, or is there a better transition point in the next 15 or 20 minutes?

MR. COGBURN: I believe I can be finished in 20 minutes, allowing approximately half that time for questions.

MR. KERR: Let's do it then.

MR. COGBURN: Okay.

(Slide.)

The next area I want to cover regarding operating performance of the CPC system, I want to cover the licensee event reports.

A licensee event report is generated as a result of the channel failure and then being bypassed. The normal practice if a channel fails, it will trip, and the operators will bypass it. This generates a licensee event report. Also, three restarts that occur in one day will also require the writing of the licensee event report.

The system -- the CPC system was designed as a two out of three system with installed spare. It was, however, licensed as a two out of four system, because there were some unresolved points at the end of the period, licensing period.

If the system had been licensed as designed, as a two out of three system, then many less than this total number of 34 LERs would have resulted; and in fact, I believe there would have been only 10 total events, 9 of those related to CEA calculators, because going into an action state when the tech spec requires generation of a licensee event report, there was one other human error that generated a licensee event report.

The frequency of occurrence of these events you can probably assess for yourselves. In '78 there were two LERs, in '79, 18. In 1980 there were 14, and so far in '81 we have not had a failure with an LER.

I broke this down into hardware failures and human errors, and I further broke down the hardware failures that caused these as either a solid failure, one that was easy to diagnose and repair, or intermittent failures. So that the intermittent failures have been identified and fixed; some of them have not yet. The human errors were primarily associated with test instrument connection which technically made one channel inoperable.

(Slide.)

The hardware failures that have occurred during reactor operation, for this purpose I used the time that the reactor has been critical, because that is the time that the core protection calculators are required to be in service.

MR. LIPINSKI: Before you start on this, on the other one you only listed the hardware failures and human error. There were not LERs involving software?

(Slide.)

MR. COGBURN: No. Software did not -- the software caused plant trips, but a plant trip does not necessarily require an LER.

MR. LIPINSKI: Yes. That was discussed yesterday. That was one of the proposed changes for LERs.

MR. COGBURN: The plant trips are reported in the monthly operating reports and the cause. This table, hardware failures, integrates the licensee event reports with the failures that have occurred that have caused plant trips; and I have broken it down to the failures that occurred by channel and by specific calculator. The number -- the total number of failures I believe comes out to 49.

I have also calculated a mean time to failure based on the hours critical and the total number of trips that have occurred, and I got an average channel availability or a mean time between failures of 896 hours based on our operating experience and its initial criticality.

MR. RAY: Is there any indication on the part of suppliers -- that Combustion Engineering requires on such a figure, the average mean time between failures of components in the system?

MR. COGBURN: Is there specification on what it should be?

MR. RAY: Does CE have a specification on its suppliers as to what they would consider acceptable?

MR. COGBURN: Bill, would you care to answer that, or Ed?

MR. BROWN: Ed Brown, Combustion Engineering.

At the time this system was designed and fabricated there were no specification values for target availability at that time.

MR. RAY: How about today?

MR. BROWN: Today there are.

MR. RAY: Can you tell us how that compares with 896?

MR. BROWN: 896 is calculated based on reactor time availability, not total operating time. When we specify the system we base it on calendar time and availability, so it is hard to compare this number without knowing the total operating time.

MR. COGBURN: We do not make any effort to -- well, when we are not operating, that's the time we shut the CPCs down and perform preventive maintenance and things like that; so there is not sufficient data to do that, I'm afraid. Failures are not specifically addressed or noted that occur other than by job order at the plant, the documentation system that we have; but I might revise that. I have not done that research. It might be possible to do it. I don't know.

MR. KERR: Mr. Pearson.

MR. PEARSON: I have a question. Have you found any unsafe failures? All the failures you're talking about are those that have either been detected because the system failed safe or a diagnostic forced it to fail safe.

Now, when you do some routine testing that's the time when unsafe failures should be uncovered.

MR. COGBURN: Okay. That really leads into what I would like to say, is one of the reasons why we believe the data links are valuable.

The most probable mechanism for such a failure to occur is an instrument drift, a non-conservative instrument drift. We have not noted that, because the sensors have tended to fail completely. However, drift has occurred, and the way we have picked up that instrument drift is by frequent logging and comparison of the various sensors and intercomparison of the systems.

Possibly there might be another way to do it, but the best way we have come up with is to have the plant reactor operators logging and comparing channel to channel by looking solely at the CPCs, their operator modules.

As an independent look I have my reactor engineers perform periodic and at least weekly trends of all of these signals simultaneously through the data links, and this is the only way that we have presently available the data links to do this.

If you trend this over a period of time, both hours, days, weeks, and look at it in various lights, you can pick up tendencies for those instruments to drift out of what your calibration error should be, and we have been successful at that so far in identifying the drift before it became non-conservative.

To the extent it was not accounted for and to be able to put the channel into a repair situation where you fix the sensor, and there is my position of what the best use other than startup testing where the links are absolutely essential to do the shape annealing matrix test and some others.

I believe there is also a necessary future of a good core follow program. Instrumentation surveillance is an important part of the CPC or any protection system surveillance to improve safety and operability. If we wait for the instruments to get way out of tolerance, then there can be an unsafe failure.

Does that answer your question, sir?

MR. PEARSON: Yes.

(Slide.)

MR. COGBURN: Let me summarize the last couple of slides on failures.

I calculated the mean time between failures per channel. This is the same number, 896 hours average. That includes the CEACs. A mean time to repair based on our experience of 1.3 hours. This includes some long times and some very short times, for it only required free initialization of the calculator.

The total number of failures peg at 49. The time that the CPCs are in service, and from 6,208 hours calculated an average channel and availability of .0017, which I believe is a fairly good unavailability.

I think there are still some improvements that can be made, but this also includes the early problems, and the performance has improved significantly since the beginning. The problems that we have had --

MR. KERR: Help me with my arithmetic. I'm having problems here. With an average mean time to repair of 1.3 hours, you ought to have about 65 hours out of service.

MR. COGBURN: This number of failures is all the channel failures, an this availability -- unavailability is per channel; so this number really is divided by six, six calculators.

MR. KERR: Okay.

MR. COGBURN: I meant to point that out. I'm sorry.

Again, the problems that we have observed ha been early on. The room cooling for the room, the CPCs in our plant are located in their own room. The initial design called for the emergency control room chillers to be the room cooling for that room. Those do not normally run to cool the control room. They are the emergency system.

The chillers, therefore, are way over capacity for the CPC room, so we found they would not run as installed. They would freeze up. They get too cold. And so we added a separate room air conditioning unit early in the operating time.

Now, this system has not been as good as it might have been, and we are still looking at changes. We are adding an alarm in the control room on high temperature, and operators would then start the emergency cooling system. We are making changes to the emergency chillers to allow them to run without tripping out on too low a load or freezing up.

But the design of the system -- and AP&L was at fault here in not determining this earlier -- must consider a good air conditioning and humidity control system, and we still have a ways to go in that regard, but we have made some progress.

We also have some power supply problems with our inverters. They had spikes on them. The design was a new one, and it required modifications. There would be power failures with the inverters. This mostly occurred before we ever went critical. But I think both the room cooling and the inverter problems have been improved.

MR. KERR: Is the inverter part of the CPC or it is not?

MR. COGBURN: No. Each PBS channel has an inverter, and the CPC is powered from one inverter. I think there is good reason to believe that the cooling problems and the inverter problems may have caused some hardware problems that we have not recovered from yet; and one of the things we are evaluating seriously is --

MR. KERR: Did you have the inverter problem because it was a new inverter, or because the CPC is especially sensitive to inverters which would be okay on an analog system?

MR. COGBURN: I think it's the inverters. The CPCs are very sensitive, that's true; but the inverters were, I believe, the fault. The problem was resolved by them, because the analog system was also affected by the inverters.

We had an inadvertent containment spray-down before -- back during hot functional testing that was related to inverters, and a lot of modifications were done before we went critical.

MR. KERR: I would like a little more information on your air conditioning system. You had said something about having a long way to go, which implies that it may be a 20-year period ahead of you to get the air conditioning system operating.

MR. COGBURN: Well, there have been several modifications that we have been making steps. Each one we hope is going to solve the problem. I don't believe it has yet, because even with a new system we have an unreliability problem, so there are two avenues we are approaching. They are not 20-year programs. They are probably 12 or 18 month programs, in my opinion.

One is to evaluate the need for a backup air conditioning system for the CPC room. Another is, as I mentioned, was to improve the existing backup, the emergency control room chiller system so that they can be a more effective backup. Making the operators aware of the situation has been our most recent change, so that they can respond quickly to higher temperatures in the room and start the emergency chillers.

So I see it as an ongoing thing. I don't believe we have accomplished where we need to be.

Mr. Epler said something about we had achieved an adequate reliability, I believe, and I'm not really sure what you were referring to; but there is a point in reliability where you say yes, that's good. I don't feel like we're there yet, but we've made good improvements.

MR. KERR: I don't think Mr. Epler was talking about air conditioners, because if there's one place where American technology has completely failed, it must be in air conditioners.

(Laughter.)

MR. COGBURN: But the air conditioning has an indirect effect on the protection system.

MR. KERR: I'd say it's pretty direct, and that's why I'm concerned that it's 18 months. It seems to me you ought to be able to fix the air conditioner sooner than that.

MR. COGBURN: Well, of course you realize when you have things in the room like that, seismic design is a problem. Electrical interferences are concerned, and you've got to evaluate a lot of things. It's not that simple. At least as I perceive it, it's not that simple. I would suspect that it would be 12 to 18 months.

MR. KERR: My only comment is it seems to me this air conditioner is a fairly integral part of the reliability of your CPC.

MR. COGBURN: Well, I'm extrapolating my own opinions here.

MR. KERR: I didn't get that from your opinion. I got that from reading the LERs.

MR. COGBURN: Right. But I'm saying we have made changes that many of our engineers believe are going to fix the problem. I'm skeptical, yes. I guess I have to be proven wrong or right, one or the other.

MR. LIPINSKI: Are the air conditioner failures total, or are you failing to maintain temperature?

MR. COGBURN: They typically are totally. It trips off. The temperature rises. It's noted eventually, and then the backup system is started. We are trying to make that recognition process more prevalent now.

MR. LIPINSKI: Is that enunciated in the control room?

MR. COGBURN: Yes. But it's in the back of the control room, and they are not very prominent. What we have added is enunciation on the cooling temperature outlet to the new parameter before we ever get to the cabinets, because there is such a lag time between -- I'm sorry.

MR. LIPINSKI: Have you described the TMI situation of information that's not available to the operator because s somewhere in the back?

MR. COGBURN: I think this is nowhere near as significant as the problems at TMI, but it is a feature that deserves some attention.

MR. LIPINSKI: Is there an audible enunciation when this temperature goes up or just visual?

MR. COGBURN: There is both now. We actually -- I'm not sure if it's implemented today, but it's very near implementation, where a new alarm and a new sensor on the outlet temperature from the air conditioner is measured to give a more immediate sensing of the problem. And this is now a front panel enunciator, audible and visual.

MR. LIPINSKI: It is now front panel?

MR. COGBURN: As I said, I'm not sure it is implemented today, but it was getting very close. The implementation is in progress on this particular item.

Other problems that we have had which the diagnostics -- the area diagnostics -- we have made one set of changes to add some diagnostics. Based on that we found they were very helpful for finding sensor failures that were difficult to track before. We found a few problems with that which we are planning to modify for cycle 2, and the San Onofre system would have the same features for additional failure diagnostics.

Still, we are having quite a few failures that we have not been able to diagnose as failures, within the IO hardware some of the peripheral equipment associated with the protection calculators. And I believe Combustion and Arkansas Power and Light have been discussing the need for additional diagnostics which we hope to add to help track down failures and make them a little easier and a little quicker to assess.

This is another feature of our improved performance. As I said earlier, I feel like the unavailability is reasonably good now, and I would like to see it a factor of three better myself; and I believe we can get there, but our priority on this has been satisfied somewhat because we have made quite a few improvements.

MR. KERR: Would a factor of three be significant?

MR. COGBURN: I believe it would be. At least -- I would like to say at least that much, maybe more, is achievable. But that would mean instead of -- you know, we'd be up around 3,000 hours between channel failure, which with the existing computer technology is, I think, we're going to be hard-pressed to beat that.

Also, as I mentioned earlier, there were some oversights in the algorithm design. These have been corrected, the software changes, and they will be described further.

MR. LIPINSKI: Before you leave your failures, one sheet showed you still had two failures in '81.

MR. COGBURN: We had two trips in '81. One of those was a rod drop, and one of them happened during a surveillance. We had no LERs but two trips. One was a protection trip from a hundred percent power rod drop. The other one was during surveillance periodic test where the test procedure specified testing the reed switch position supply over logic, which required powering down one reed switch position transmitter.

Apparently -- and this is not completely analyzed yet because it only occurred last week -- but apparently that didn't function, and we found it by the periodic test, and we suffered a trip because of that.

MR. LIPINSKI: That was a legitimate trip due to a system failure?

MR. COGBURN: I would call it a non-valid failure. The rod drop was a valid failure. This one I would call a non-valid failure. We know the reason or we think we know the reason for it and can correct it. However, it still occurred.

MR. LIPINSKI: So you're still uncovering problems with this system as you gain operating experience.

MR. COGBURN: Yes, sir. I'm sure we will always continue to uncover problems, because we have to determine what the expected life of the components is.

MR. LIPINSKI: No. I'm thinking of -- the one you just described --

MR. COGBURN: No, sir. I don't consider that design. It's a hardware failure.

MR. LIPINSKI: The numbers -- there are two numbers of interest. One is the failure rate that leads to undetected failures. This number is not, because you said you have had no undetected failures; so all your operating hours to date go in the column with no failures or unsafe failures. These numbers here are for your safe failures which are leading to spurious trips.

MR. COGBURN: Yes, sir. Invalid trips.

MR. LIPINSKI: Right.

MR. COGBURN: These numbers are spurious, yes.

MR. LIPINSKI: The reliability of the system is generally associated with the probability of getting a failure on demand, and that number looks excellent with no unserved figures recorded; so from an operational standpoint you are being plagued by the safe failures.

MR. COGBURN: I think our belief is this is availability of plant performance concern and certainly not a safety concern.

I will wind up in about two or three minutes except for questions that occur.

I think the things I would recommend that need to be followed up on and factored into new designs, or in other words what I would change, we need a solution to the one out of two protection problem. ANO-2 is the first of a kind to get that protection system, and this is an action item that

AP&L and Combustion Engineering needs to address, but I think the industry needs to address, because if CEA input is going to be used, and it apparently needs to be used -- the other reactor vendors are going this direction also -- then the one out of two system needs to be resolved from a reliability standpoint, not from a safety standpoint.

This system should be -- and we intend to pursue licensing as a two out of three systems deal versus two out of four. It was designed to be a two out of three system. Many other power plants that I am aware of are licensed as three-channel systems. Our Unit 1 is a three-channel system with an installed spare.

A couple of other things that I have checked with San Onofre about to make sure they don't have this problem, but we ended up locating our core protection calculators in the radiation control area. This makes them a little more difficult to maintain and is not desirable, and their temperature and humidity control seems to be much better thought out than ours was. They are located in a regular control room environment.

MR. KERR: Considering the relative reliability of air conditioning systems in this country, they might want to consider putting them in a refrigerator.

MR. COGBURN: One thing that's critical with this system and anyone that uses data link information, and data links are installed between the CPCs and CEACs, is that steady temperature and humidity is desirable. The oscillator frequencies will vary and the cable resistances vary, and data linking errors can result.

Some of our problems are related to that. Some of these unknown problems I believe are --

MR. KERR: I noticed in one LER that you lost a bit, and I was curious as to how you noticed that, but I won't pursue it.

MR. LIPINSKI: How sensitive are these temperature changes? Are we talking about 50, 60 degrees or 5 or 10 degrees?

MR. COGBURN: On the order of 10 to 20 degrees.

Evaluation of the CPC system, in summary, I believe that it is very fail-safe, and the fuel protection provided by it is very good. It's probably the best in the industry in that regard.

Fuel failures are a real problem in the industry, and I think the CPCs and the monitoring systems in the ANO-2 and later designs are probably the frontrunner in the industry.

The software in my opinion is very good, and the display features are extremely good. The human factors design is good, and the quantity of information is very helpful to the operators.

I think the hardware still needs further improvement but is adequate, and again, the one out of two system for CEA inputs is hurting our availability.

And that's my summary of the CPC system. I'm ready to close except for questions.

MR. KERR: Are there questions?

MR. LIPINSKI: I have one question. If you have a spurious trip, how quickly can you restart in terms of what your average down time amounts to?

MR. COGBURN: It typically takes 24 hours to get back on the line.

MR. LIPINSKI: You lose one day?

MR. EPLER: It's one day a month.

MR. COGBURN: Yes.

MR. LIPINSKI: Are you associating power cost with one day yet?

MR. COGBURN: The power cost for one day for our system are on the order of half a million dollars, the replacement power cost, and financially that is very -- in the rate structure in Arkansas that hurts AP&L pretty badly, because if the availability is below a specified number, then we pay all the difference to buy fuel and to replace the nuclear generation.

MR. LIPINSKI: So you have an economic incentive to make an investment to improve this availability.

MR. COGBURN: We have a strong economic incentive, and our engineering and operating staffs have a strong management pressure -- we feel a strong management pressure to improve the system because of that.

MR. KERR: Mr. Boyd.

MR. BOYD: May I just ask a question for clarification? Does a control rod drop cause a trip or only through a DNBR or other calculation?

MR. COGBURN: A control rod drop will cause a one-channel trip almost directly. It will cause a plant trip only if its deviation is large enough and its worth or effect on power distribution is great enough to cause a large penalty factor to be generated by the two CEA calculators and then transmit that penalty to the CPCs which apply it to the DNBR and local power density calculations. So it is an indirect plant trip. It is essentially a direct channel trip. If one of the rods is designated as a safety rod bank, that will cause essentially an immediate trip of one channel.

MR. BOYD: I don't understand, therefore, why you had, I gather, several plant trips due to rod drops at low power.

MR. COGBURN: Well, this is because in the initial design there was only one penalty factor essentially for a rod deviation, and it was the worst case rod deviation, and it was a very large number.

Mr. Bozek will describe this quite a bit further. I believe. Yes.

MR. KERR: Are there other questions?

(No response.)

I declare a recess until 1:40 p.m.

(Whereupon, at 12:40 p.m., the meeting was recessed for lunch, to be reconvened at 1:40 p.m., the same day.)

AFTERNOON SESSION

(1:40 p.m.)

MR. KERR: We come, according to my interpretation of the agenda, to a section called "Software Changes to the CPCS," and I assume that's going to be handled by CE.

MR. KENNEDY: That's a correct assumption, Dr. Kerr. Our next speaker is Mr. Tom Starr. Tom is the supervisor of our CPC design group, and he is going to cover the software change process.

MR. STARR: Mr. Chairman, the purpose of my presentation is that prior to remarks by Rozek this afternoon on the software changes that have been made to Arkansas and are being made now to SONGS, I would like to present the software change process that occurs when we make such modifications.

This is the process of implementing the software changes as dictated by the functional designers and placing that design into an assembly language code.

(Slide.)

CE has developed a highly structured and detailed software change process, and this process was documented in the software change procedure called CEN-39, which was also referred to this morning.

CEN-39 has been approved by the NRC staff during a resolution of staff position number 19 during the ANO-2 review, and that was completed in mid-'79.

CEN-39 has been followed for all ANO-2 and SONGS software changes, and its fundamental approach has been used for the original ANO-2 design, so that for the current SONGS and Arkansas work, we are at the fourth time for using this procedure; and the following discussion covers several important features of that software change process.

(Slide.)

To ensure that the process of specifying and implementing the software modifications is done in a manner that maintains the integrity and reliability of the software is the purpose of this CEN-39 process. When we go into change the software we want to be absolutely assured that we are introducing no new errors and that the functional design is correctly implemented.

The scope of the process includes the functional design, and by functional design I mean specification in algebra to the assembly language programmers of the programs that we want implemented. That includes data also. At the stage that the functional design is complete, one could take that design and implement it in any computer or language that one would choose. In this case it's Perkins-Elmer equipment, and it's been done in an assembly lab.

The idea of functional design is that it's an engineering design. It's based on engineering analysis and completed prior to implementation.

Software coding and implementation is also covered in this procedure, as is the software testing. All documentation related to functional design, software coding and implementation, and testing is covered by this procedure.

A wide spectrum of detail is included from a relatively high level of requirements from this system down to very precise, specific instructions for generation of listings and so forth.

The applicabilty of CEN-39 is that it is applicable to all software changes, no matter how minor.

MR. KERR: Could you tell me what is meant by the first statement on that slide, please, sir?

(Slide.)

It strikes me as being a rather qualitative statement.

MR. STARR: To a large degree it is a qualitative statement. We're striving to ensure that what we change, we change correctly, and what we do not intend to alter, we do not alter.

In the testing that we have done to date since we have been making modifications, we have found a relatively few number of errors.

MR. KERR: Let me be more specific. Is your goal to set up a procedure that will eliminate errors, or do you have as a goal a procedure that will make the probability of errors smaller, or do you have some sort of quantitative goal?

MR. STARR: It's a matter of making the probability of errors acceptably small. We not have a quantitative data base to which we are striving.

MR. KERR: How do you know when you have an acceptable procedure other than that the NRC approves it?

MR. STARR: Well, we are quite satisfied with it.

MR. KERR: Well, I'm not being facetious since you're willing to stand back of it, but how did you -- what criteria do you use to conclude that your procedure is a good procedure? I think it isn't just a change in software; that what you're concerned about is validity of software generally.

MR. STARR: I think it's a matter of the constructs of this software itself, that is, modulization. It's a matter of keeping all documentation current. It's a matter of what we consider --

MR. KERR: I have difficulty believing that documentation produces anything except documents.

MR. STARR: Well, it helps keep the probability of errors acceptably small.

MR. KERR: Well, it does if it's good documentation. I'm trying to get a feel for how internally you conclude that your procedure is one that will produce results that you want to achieve. Is it just a matter of somebody sitting back and saying well, now, I have this quality assurance program, and this documentation, and these good people; I must have a good procedure?

MR. STARR: It is a matter of judgment, and that judgment is made by engineers and programmers; and that is about all I can say.

MR. KERR: So aside from faith in the system, I really don't have any very objective criteria?

MR. STARR: We have not done any qualitative evaluation of our success and our goals.

MR. KERR: Do you have any outside group -- I don't mean necessarily outside of Combustion, but outside of your own immediate group to look at this and say from our perspective this is the way we think you should go, or perhaps there are some changes that you could make or some pitfalls you might avoid?

MR. STARR: There is a current draft standard generated by IEEE in the ANS group, I think, which is outside CE. We believe that we meet or exceed what is in the standard, but we do not have an outside organization currently reviewing what we do, if that's what you mean.

MR. KERR: Again, when I say "outside," I don't mean outside Combustion but outside -- there must be a number of places in Combustion where people are concerned about software reliability.

I raise this question because my own limited observation is that people don't know very much about how to make sure the software is reliable; and I'm trying to understand what approach you used.

I'm going to defer to Ed Brown.

MR. BROWN: Dr. Kerr, there are essentially two ways that we measure the software success of our system. One is in the efficiency of the procedures. In other words, we measure the effectiveness of our procedures by seeing its operational benefit.

The systems that we have implemented changes in, we have discovered no errors in the software through continued operation. So that is a quantitative measure of the acceptability of procedures.

In cases where we have discovered an error -- for example, in the original design of the system, initialization, we factored that into our original procedures and our testing program to make sure that type of error would be gone by the original software change procedures, so we have a type of feedback based on operational experience.

MR. LIPINSKI: Is there any redundancy in terms of having something go down two paths and then comparing it?

MR. STARR: Yes, there is. That occurs or the comparison occurs during testing, and I will explain that in a few moments.

MR. LIPINSKI: By your particular system as well as Fortran's comparison?

MR. STARR: I was going to explain the Fortran in comparison.

MR. EPLER: I have a question. When you have a few hundred years of light-water reactor operation, in a small fraction of those we embrace the two-unit operation; yet, we have had several cases where an operation has been performed in the wrong unit with disastrous results.

Now, I don't care how smart we are in getting the software; we can still have an awful time. How do we know that you will never get an operation on the wrong generating unit? Somebody off somewhere gets a job to put on the software, but he puts it on Unit 2 instead of Unit 1. How do we know?

MR. STARR: In the case of Arkansas Nuclear Unit 2, of course Unit 1 is not a CPC plant, but Unit 2 is; so I think for Arkansas that problem does not exist. In the future where CPC will be shipping software discs to multi-unit plants we as yet do not have a feature in the procedure that covers that possibility. It will occur in the future.

I think that is a matter of administrative and QA procedures on CE's part, as well as the positive assurance that at the other end, the utility's end, those QA procedures and administrative efforts are also made.

There are ways to assure through software that that does not happen. I think we can implement those ways as a positive assurance that that possibility you were referring to doesn't happen.

MR. EPLER: Do you believe this problem is being anticipated?

MR. STARR: Quite frankly I have not thought of it. I will defer to Ed Brown again.

MR. BROWN: Mr. Epler, we have given it thought. We have a formal configuration for each generating unit. It is essentially the same for hardware and software, because the problems are identical. The problems of making the wrong hardware change in one unit, for example, the wrong constant, are the same as making the wrong software change.

We do have a configuration, a hardware and software management plan which is essentially a design administrative control to assure ourselves that the proper hardware changes and proper software changes are made to the correct unit, unit by unit. That is proceeding.

MR. LIPINSKI: Given that you have a software change and you go through your change procedure, do you then issue a test procedure such that software can then be checked after it's loaded into the actual system in plant?

MR. STARR: Yes. There are installation procedures and checks made at the time the software is installed in the plant. They are designed as a more or less double check of the correctness of the software after it is installed. However, before we ship the hardware to the plant, we have extensive testing to assure ourselves that the implemented design as it leaves CE is correct.

The fundamental thing we are trying to do, I think, in testing is to look at two different things. One, did you design the algorithms correctly; and two, did you implement them correctly?

Our tests are separable in that generally tests are designed to do one and only one of those two things, to look at the design or the implementation.

MR. LIPINSKI: Proper tests in the plant should uncover both of those if you're going to have a functional requirement in terms of whatever that software was going to do, and if you design your testing plan properly, it should cover all errors.

MR. STARR: The reason we have gone this way is that in searching for software errors we have to be very precise. You are tracking down milliseconds on occasion. You are tracking down numerical errors on the order of --

very small numerical differences. And when you get into an in situ condition where you either have to -- you generally have to use the plant hardware or bring your own test hardware to the plant, it turns out that the inputs you need to generate to produce an output are much, much less precise than you can do in a more controlled environment in your own laboratory or on your own system.

It has been our experience that software errors were much more readily caught when they are done with special test software or with special tests that are done before the software leaves the site.

Now, of course, you can never be sure that your software shipped to this plant is perfect. You can test and test and test and be very sure that your errors are not going to impair safety, but even when you ship it, you want to test at this plant to be sure as a double check that the system is performing as you predict it should perform and that there is no overt evidence of any further problem. But once it gets to the plant, your best chance of catching software has essentially been passed.

MR. LIPINSKI: Let me summarize what you have just said, and that is that your in plant test procedures have certain shortcomings. Does this imply then that you should look at improving the ability to test in plant?

MR. STARR: I'll defer to Bill Gill.

MR. GILL: What we're saying is we do not find it practical to ship a number of people to the site or test equipment at the site to test the overall equipment. We look at this as a high technology test best done in the lab, not in the plant. There's nothing unique here. We test many components in a factory before we go to the plant.

What we are attempting to do in a plant test is to assure that those aspects which we cannot achieve in a lab, such as specific plant signatures, the impact of say the actual process noise and other signals, are tested at that point, and that nothing happened to the software from the time it left the factory until it was installed in a plant; it did not get altered in any way, nor was it changed.

So we implement the field procedures to assure that there were no changes to that disc or that software during the transport from the factory to the site.

Those aspects which we could not achieve in the lab, that actually require live plant signals, that testing we do in the plant. We divide the overall test program between the factory and the lab or the site based on practical considerations of economics and where we can best prove our goals.

MR. LIPINSKI: Your checks on the software will pick up single failures, but if you have got double-fit changes, I don't think this is one hundred percent effective, is it?

MR. STARR: I'll defer to Ed Brown.

MR. BROWN: Ed Brown, CE.

The error-checking hardware from the disc load into the system has a probability of error or about 10^{-9} per bit. That's a multi-bit longitudinal redundant check. The check signs are a further verification of loading bit by bit in the core memory.

Following that, the input-output testing provides the final verification that the software is correct. There is a higher degree, in my opinion, of certainty that the soft wiring of the system is correct than the hard wiring. In other words, there is a much more controlled environment, much more stringent testing over the installation of software than there is over the wiring of the system in any particular plant installation.

MR. STARR: I'd like to cover some of the documentation that goes with the disc for the CPC system.

(Slide.)

MR. OKRENT: The documentation is categorized for purposes of discussion in three general areas: design specification, which is generally what I refer to as functional design; design implementation, which is documentation that covers the assembly language, implementation of the system; and documents related to testing.

The design specification is based on analysis, use of the FORTRAN code to determine that the functional design, when implemented, will meet all safety requirements for the design basis list of events for the system: rod drops, losses, low power, changes and depressurizations and so forth.

This information is passed to assembly language programmers in the form of functional design specifications or functional descriptions -- they go by either name -- and basically a data base document that goes with it. The functional design specification covers basically the algorithms and the data base document covers those data that should be inserted into the program.

The software specifications cover assembly language, flow charts and equations that are implemented in the software. And the testing documents cover two types of testing, phase one testing and phase two testing, which I will explain in a moment.

The test case documents you see here are documents which are used to test modules of the software. Phase one and phase two test reports are written and the disc is accompanied by disc and test certification analysis which certifies that a large body of this work was done.

As you say, documentation cannot assure lack of errors, but it is important and we do take a lot of care with it.

MR. LIPINSKI: How is it organizationally divided in terms of responsibility? Are we looking at different groups that are involved in design specifications, implementation and testing, or do we have overlapping of activities or feedback?

MR. STARR: In general, the design specification is done by engineers who are familiar with the design basis of the system in terms of what response times are required. They design the algorithms based on NSSS design codes. That is to say, the algorithms have to be sufficiently accurate and rapid to produce a trip in time to prevent safety limits from being violated.

Their work is embodied in functional design specifications, which are then passed to, in general, the group which does the assembly language program and who are not as familiar with the design basis of the system. At that point it's being implemented.

When we do testing, for the most part phase one testing involves test cases performed or determined by programmers, and the testing is supported by engineers or functional designers. When we come to phase two testing, it is a system level test, administered for the most part by engineers who are familiar with the functions.

MR. LIPINSKI: That's the point I wanted to touch on in terms of the feedback. Are the people that were involved with the initial design specifications the same people that are looking at the test procedures, to see whether these functional specifications are being supported?

We are not dealing with static systems here. These are dynamic systems, so that the test procedures are very important.

MR. STARR: Could you repeat your question?

MR. LIPINSKI: You have a group of engineers doing design specification. Are they the same people looking at the test procedures that are used to verify the performance of the system?

MR. STARR: Yes.

MR. LIPINSKI: Okay. So effectively you have got feedback.

MR. STARR: Yes. It's not uncommon in design and testing for a programmer to say, during a test to say, we have a problem, I'm not sure if it's a bug or if it's a design problem. And you go to an engineer and you say, can you help me solve this.

So there is feedback. We are continually seeing how this process works and basing our work on our experience.

MR. LIPINSKI: Well, it's more than an engineer. It's got to be a specific engineer that understands the nuclear performance.

MR. STARR: Correct. I was referring to someone familiar with the work, yes.

MR. LIPINSKI: Thank you.

(Slide.)

MR. STARR: This block diagram gives further information on the process that we have just been talking about. On the top you will see a series of what I will call recorded calculations. In the middle you will see that these calculations are input to both functional descriptions and to data base document.

And work above that line is what I will refer to as functional design. These calculations, as I say, are both associated with design of the algorithms and data.

They are done by engineers and analysts, who base their work on the safety requirements and design basis of the system. These calculations are referenced by the functional descriptions and the data base document.

And I might add that the functional description is a complete description of the system. It includes all system level requirements, in addition to the algebra of the algorithms. And by system level requirements, I mean the configuration of the system, the timing, permissives, interlocks, alarms, annuhciators, man-machine interface requirements, and so forth.

So it is a fairly comprehensive document.

At the point these documents are generated, they are then used in software as referenced by software design specifications covering assembly language programming. From those specifications the discs are generated and sent to the site.

In addition, we are generating phase one and phase two test reports. And I will explain phase one and phase two testing in the following slides.

Phase one testing is designed to implement the changes to the CPC software, and the implementa:ion is the translation of system functional requirements in the modules of machine executable code and the integration of these modules into a real time software system. This is strictly a software test. It is done on individual modules of code.

Any module that is changed or modified is tested. Any module that accesses updated data constants is tested, and test cases are selected to exercise all branches of any module that has been modified.

After phase one testing is completed, we do what we call phase two testing. Phase two testing is performed in a single channel CPC-CEAC system located in Windsor at the CE offices.

I might add that this system includes an input simulator with analog and digital generation equipment, an FM tape recorder and various other recording equipment, such as a strip chart recorder.

Our objectives are to verify that the modifications have been properly integrated with the CPC and CEAC system hardware, and to confirm that the static and dynamic operation of the system is as we predict with the FORTRAN code. As I say, the basis for the comparison is the FORTRAN.

Item 3 should be basis for comparison is the CPC-CEAC FORTRAN simulation code.

The phase two tests that we performed are called input sweep dynamic software verification tests, or DST, and live input single parameter, or LISP, tests.

(Slide.)

MR. LIPINSKI: Could you expand on each one of those?

MR. STARR: Yes, I will.

One of the characteristics of our testing comparison between the FORTRAN and the Perkin-Elmer equipment that we do testing on is that they are different machines, and we want to know, first of all, what is the inherent difference in the processing of the algorithms based on machine difference. And we call those processing uncertainties.

The Interdata 716 is a 716 machine. The FORTRAN code i. run on a CDC 7600, which is a 64-bit machine. So we want to do two things. We want to find out if there are any small differences based on machine, and we want to verify over the operating space that these algorithms can initialize without any abnormalities.

We run a minimum of 500 test cases, and these test cases are selected based on judgments associated with the type of modification that we are doing. If we modify hypothetically the program, we will place more emphasis on flow-related test cases.

It so happens in cycle one, the current version was tested with 2,000 cases for the CPC's and 1200 cases for the CEAC calculators. We intend to run the same number for the San Onofre software.

This is a static, steady-state test. The dynamics involved only relate to the initialization.

(Slide.)

Following the input sweep test in phase two, we run the dynamic software verification test. This is a dynamic test that is intended to properly assure the dynamic response of the system and further assure the correct software implementation -- we run a minimum of five test cases.

Example cases are the followihg design basis events: a four-pump loss of flow, a single CEA drop, control bank withdrawal, rapid depressurization, and an increasing power ramp. These cases are designed to be as much like a real basis design event as we can make them.

It is strictly a software test, and we have found it to be very useful in detecting software errors.

MR. LIPINSKI: Now, the inputs for these test cases come from analog test?

MR. STARR: No, they do not. They are established by special software. And the reason we do that is when you are comparing a FORTRAN code to the assembly language code you want to be very, very precise in getting the inputs exactly the same with respect to time for both systems. So we do that with software.

A special disc has these test cases on it. They are loaded in a memory and the transient is initiated, so that the inputs versus time are exactly the same, which enables us to see more clearly any software errors that the outputs versus time are not the same.

MR. LIPINSKI: How is that disc generated?

MR. STARR: It is generated by our software group. The test cases are selected by engineers who are working on phase two testing. The process of generating that disc, I believe, is in accordance with CEN-39, although I don't know for sure. I'm getting a yes from Ed Brown.

So the disc generation process for this software is as rigorous as it would be for the actual software.

MR. LIPINSKI: Somewhere you've got something that is generating a full characteristic that's gone onto that disc with digital values at discreet time increments that would correspond to a real time event in the plant.

MR. STARR: That is correct. If you're asking how we select test cases --

MR. LIPINSKI: No. How you're generating the test cases. Somewhere you've got something generating on your digital computer, that is in turn producing --

MR. STARR: For the most part, the NSSS design code we use is C-SEC. However, we do have other codes we may choose to use. But in general, C-SEC is the one that we use. It is a full-scale NSSS design code that simulates the

RCS, steam generators, core pressurizer, and so forth.

MR. LIPINSKI: Then you bypass your analog-to-digital converters on the input to the actual system and put it in the digital banks?

MR. STARR: That's correct. This test does not include analog-to-digital conversion. And as I say, the reason we do that is we want to be very, very precise.

(Slide.)

The third part of phase two is called the live input single parameter test, and this test does include analog-to-digital conversion. Its objectives are to further assure the dynamic response and the implementation of the software, and to evaluate the dynamic response of the input hardware and software together.

We have a minimum for the five test cases that are required for any case. The example cases are pump speed ramp, the ex-core detector signal ramp, temperature signal ramp, pressure signal ramp, and single CEA signal ramp.

The reason that we include, of course, the analog to digital hardware here is that we did not do it in a test and we want to make sure that we exercise those inputs during our testing.

(Slide.)

The message, then, or summary that I want to leave you with is that we do have a highly structured and detailed process; staff reviewed that process in CEN-39 and concurred; and that we are applying this process to the Arkansas changes, and that we will be applying it to others.

That completes my presentation. I will take any further questions.

MR. LIPINSKI: Question. If I go back to your dynamic software verification, I see changes in plant parameters that may not be singular, although I guess if you only got flow all you're going to generate is a flow signal, no changes in the temperature signal; is that correct?

MR. STARR: These cases are based, as I say, as nearly as we can make them on our simulation code results. And I think for loss of flow in the time scale of that event, temperature changes are very minimal, if anything. It's a very rapid transient.

MR. LIPINSKI: But the question is, what's on the disc? Are all the measured parameters on the disc that the system would be sampling?

MR. STARR: Yes.

MR. LIPINSKI: So your simulation would develop the change in all parameters, if they should occur?

MR. STARR: Yes.

MR. LAWROSKI: And now, if I go to your other cases, you only have a single parameter being changed at any one time.

(Slide.)

MR. LIPINSKI: You do not generate an FM analog tape with all parameters changing for the test cases. Well, in these particular test cases they can't, the reason you selected them.

MR. STARR: The reason we used the single-parameter ramps again goes back to our objective of changing software errors. It's our belief that if you drive the system with a lot of things changing at the ame time, your ability to isolate software errors can be affected. We would rather go down and select a single signal, particularly here where we were dealing with input with analog-digital conversion. We'd rather select a single signal and drive the system with that signal, and examine with particular care those areas of the code that are affected by that signal, so that we can better isolate any possible software errors. That's our objective.

MR. LIPINSKI: Well, that's fine. You've picked out your first five initial test cases. But there's nothing that says that the list cannot be continued.

MR. STARR: That's true. I might add, in terms of continuation of testing, I might add on DSVT, we do run much more than the minimum. And I think the signals have been, in our experience, pretty informative in terms of driving the system. You can make a lot of things happen with just one signal changing.

In answer to your question, yes, the list can be made longer. And if in our judgment it should be, we will. Each time we do a test, we take a look at what we are doing and don't follow the procedure blindly. We do make an ongoing evaluation each time of what it is we are doing.

MR. LIPINSKI: How do you know you're not getting into trouble with sampling rates and data transfer, when you are operating in real time, if you only do one of these single parameter bases?

MR. STARR: I don't quite understand the question. I think Ed Brown would like to speak, so I will defer to him.

MR. BROWN: Dr. Lipinski, we have designed the system to have a very simple sampling structure and data transfer structure, such that it can be completely analyzed and predicted. The DSVT test, reading the perfect inputs, simulates all of the sampling rates and data transfer rates that you would see in real time.

So that if there were an error in the system, it would be at that time detected.

MR. LIPINSKI: If I recall, this is implemented in the floating point?

MR. BROWN: Right now, with all the changes we have made, all of the CPC changes are implemented in the floating point.

MR. LIPINSKI: So you don't have to --

MR. BROWN: That's correct. One of the changes that Mr. Rozek will talk about later on is that we did have in an earlier version the flow algorithm in fixed point, and we made a conversion of fixed point based on what we thought was an increase in overall reliability of the system for that consideration.

MR. LIPINSKI: Without the floating point, you have the same results you had in --

MR. BROWN: That's correct.

MR. KERR: Another question?

MR. BELTRACCHI: My name is Leo Beltracchi.

In regards to your question, the examples of the single variable transients, the staff in its original review with the core protection calculator system required that these be done in single variable, in order to test a specific dynamic algorithm. And the only way you could really assure that you could achieve this was by initiating that variable, the key values for that algorithm, in a single manner, rather than attempting to incorporate the changes of all variables simultaneously.

MR. LIPINSKI: One thing that's bothering me, what are there, eight inputs typically in terms of temperature, pressure, flow, flux?

MR. STARR: If you include the CEA's, you're up to about 30.

MR. LIPINSKI: Not each CEA individually, but generically.

MR. STARR: Well, generically, you have ex-cores, temperature, pressure and CEA, I believe generically, unless you want to break down temperature in the cold leg and the hot leg. But if you don't, then you have five inputs here.

MR. LIPINSKI: But for each of these five inputs, I have a magnitude. If I want to think of this as a vector set, I also have a rate. So I would have ten variables as an input that I can assign initial conditions to in order to initiate a transient into the system.

MR. STARR: Five initial conditions and five rates.

MR. LIPINSKI: So I have a ten-variable set that I can walk off into a vector space and go from all corners of this space to make sure that I'm not having trouble in getting the information processed through the system to generate output signals.

MR. STARR: Correct.

MR. LIPINSKI: I'm still not convinced that you can walk in any corner of the space that represents a reasonable starting point of linear transients and guarantee that you generate the required output.

MR. STARR: We do not run dynamic tests all over the operating space. We select our cases based on our experience and judgment.

I would remind you that the input sweep test, which is a very large set of static test cases, shows that initially we have implemented the software correctly, at least in a steady-state sense, so that each point in operating space can initialize and gets the correct answer.

Dynamically, we do not do that.

MR. LIPINSKI: Static cases only take care of the magnitudes. It does not take care of the rates.

MR. STARR: That's correct. We choose our rates for the --

MR. LIPINSKI: Individual parameters.

MR. STARR: Individual parameters, yes. But we do not go all over the operating space with them.

MR. KERR: Are there other questions?

(No response.)

Can you think of anything within your experience that has been of value insofar as where you now are on this procedure, that has made a significant change in what you do or what you look for?

MR. STARR: Not with regard to the ANO-2 operation. But with regard to our early testing of the software, I would again point out that we found it best to separate the goals of testing for functional adequacy, just to separate that goal from the goal of testing for correct implementation.

If you try to set up a test that is trying to do both at the same time, it seems to detract from each goal. And it appears best to us to look at each one separately.

I would defer to Bill Gill.

MR. GILL: There are two major learning experiences in terms of software testing from the first, say, two years. One is our original approach to testing was to have one processor, and you figure that is either a CPC test and then you can figure it as a CEA calculator. So we did not have the ability to test the interaction between the CEAC and the CPC.

As Mr. Cogburn had mentioned earlier, one of the design problems we had was an interaction problem. Today we have a CEAC and CPC with the data link as part of our single channel. So it was a lesson learned. We have upgraded to single channel.

The second major change we made is we previously ran the input sweep, which to us is the test that gives us the most confidence, only on the CPC. The CEA calculator was a simplified software structure, and we were confident we could analyze it by inspection or testing, other than input sweep.

Based on the changes that Tom Rozek will talk about, we have increased the complexity of the CEA calculator software and its sophistication is such that it approximates, although much less, the CPC. In response to the additional complexity, we have input sweep testing on the calculator. So we have significantly increased our test ability of the CEA calculator and the CPC in the last year.

MR. KERR: Mr. Brown?

MR. BROWN: There's one other thing we've learned from the software engineering aspects, and that is that the testing that we have is extremely sensitive. We were able to detect differences in the hardware implementation between the 716 and CEC 7600, specifically in the way in which they handled floating point numbers.

Our test criteria were so sensitive we thought we had a hardware error until we modeled the actual floating point hardware of the machine. And the test was so sensitive we could see the differences.

MR. KERR: Do you have a mechanism that will continue to follow the operation of this equipment, so that if lessons do show up or things do show up you will be in a position to learn from it?

MR. BROWN: Yes, we do, sir. We have two mechanisms, two formal mechanisms. One is a field action

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

-

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON ELECTRICAL SYSTEMS

TO REVIEW MATTERS RELATING TO

THE USE OF COMPUTER PROTECTION SYSTEMS

Nuclear Regulatory Commission

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

February 24, 1981

The subcommittee convened, pursuant to notice, at 9:00 a.m.

ACRS MEMBERS PRESENT:

W. KERR, Chairman
J. C. EBERSOLE
J. J. RAY

CONSULTANTS PRESENT:

S. DITTO
E. EPLER
W. LIPINSKI

DESIGNATED FEDERAL EMPLOYEE:

R. SAVIO

ALSO PRESENT:

H. ALDERMAN
F. BOYD
A. PEARSON
B. MORRIS
L. PHILLIPS
M. SRINIVASAN
E. KENNEDY
A. SPINELL
T. COGBORN
T. STARR
T. ROZEK
B. GILL
W. MOODY
E. BROWN

* * *

request from our utilities and the other is our corrective actions program, which transmits data such as LER's and indications and things like this back to the designers.

And there is also the informal communications right in the utility. We constantly factor back in our operating experience and our design.

MR. KERR: Thank you.

Mr. Lipinski?

MR. LIPINSKI: On your ramp signals, who specified the ramps? What people in your organization?

MR. STARR: Engineers associated with the functional design of the system.

MR. LIPINSKI: So it went back to the front end, where it was specified?

MR. STARR: Phase two in general was administered by engineers associated with the functional design and analysis of the system. Phase one in general was assembled by assembly language programmers.

MR. KERR: Does that complete your presentation?

MR. STARR: Yes.

MR. KERR: Thank you, sir.

MR. STARR: You're welcome.

MR. KERR: Is that part A of number 4?

MR. KENNEDY: That was part A of number 4. Part B and C of item number 4 will be presented by Mr. Tom Rozek.

Mr. Rozek is the cognizant design engineer for the calculators, and he has the enviable task of responding to all the questions we've been putting off all day.

Mr. Rozek.

MR. KERR: His last name is spelled --

MR. KENNEDY: R-o-z-e-k.

MR. ROZEK: Good afternoon.

(Slide.)

I would like to divide the software modifications into two areas. The first area is based on the changes that were made during Arkansas Cycle 1 operation. We made two sets of software modifications based on operating experience at Arkansas.

The second area of modifications are those that will be implemented SONGS 2 above and beyond those made in Arkansas Cycle 1. In addition, these modifications that we are making for SONGS 2 and 3 will be implemented in ANO-2, Cycle 2.

(Slide.)

Since I have a tendency to talk in acronyms occasionally, I have provided a list of acronyms, and I hope they are helpful for you.

(Slide.)

ANO- is the first plant with a CPC system. The original software, since it was a first of a kind design, the first plant with a digital protection system licensed in the United States, the original software was conservative. This conservatism impacted plant performance during Arkansas Cycle 1 operation.

During Arkansas Cycle 1 operation, we made two sets of software modifications. The first set which I will call Mod 1/2A or Mod 1/2A, was implemented June 24th, 1979. These changes were based on the early software qualification and testing, original phase one and phase two testing, and early ANO-2 operation, before Arkansas reached about the 20 percent power plateau.

The second set of modifications, called Mod 2B/3, were implemented in May of 1980, and these changes were based on later ANO-2 operation, feedback we got from AP&L, and a rough breakdown on that would be about 50 percent power, that we gained from Arkansas operation before they had 50 percent power.

The notation Mod 1, Mod 2, and Mod 3 are just notations that CE and AP&L have agreed to in defining these changes. They are sets of changes. We have three sets defined. We implemented 1 and part of 2 at one time, and the rest of 2 and part of Mod 3 at a later time.

Both sets of software modifications were made in accordance with the software change procedure CEN-39, which was discussed by Tom Starr.

MR. KERR: Just as a matter of curiosity, is the word "impacted" a pejorative term?

MR. ROZEK: Could you repeat the question?

MR. KERR: Is the word "impacted" as used in 1B considered a pejorative term?

MR. ROZEK: I don't know what that word means.

MR. KERR: Well, is "impacted" good, bad or neutral?

MR. ROZEK: In this sense, it would be bad. It caused spurious trips at Arkansas.

MR. KERR: Thank you.

(Slide.)

MR. ROZEK: In a diagram to show where these changes have been made, and with Arkansas Cycle 1 milestones, I have provided this slide. Initial fuel load was in July of 1978. Initial criticality was in December of 1978.

About eight months or seven months later, in late June, we implemented the first set of CPC software modifications. In late January of 1980, ANO-2 first achieved 100 percent power.

About five months later, we implemented the second set of software modifications, Mod 2B/3.

Arkansas is planning to shut down late next month for the end of its first fuel cycle, and beginning of a second fuel cycle is predicted or hopefully predicted in the middle of May or the first of June.

(Slide.)

What I'd like to present is some of the software modifications that we did make for Arkansas Cycle 1. I don't plan to go into a lot of detail on these changes, but I will go into detail on the changes that Mr. Cogburn brought up that aroused some interest, and I'll talk about those in a little more detail.

And I will talk about what I consider the more major changes we presented to the NRC staff last May.

The first change was we made changes to the low power fixed ex-core shape in the CPC's. The CPC determines power distribution from the ex-core signals. At low powers, because of zero or near-zero ex-core signals, it cannot calculate the power distribution.

So the CPC uses a fixed power distribution. In the Arkansas Cycle 1 design, we had a couple of problems with it. The first was the chattering about the breakpoint, above which the fixed ex-core shape was not -- the real shape was used, and below which the fixed ex-core shape was used.

You don't have this slide because I just added it.

(Slide.)

But our objective in this change was to preclude the excessive conservative values of DNBR at low power because of the switching between the shapes. We had a boundary point. We had no histories. The previous design for powers lower than at breakpoint, as I said, we used the fixed ex-core shape in the power distribution calculation. Above this breakpoint, we used the actual power shape.

The changes that we made in this area -- Tom Cogburn brought up that this problem did cause us what he called "a design error," in quotes, that was the result of one reactor trip at Arkansas. We made three changes in this area.

We made the fixed ex-core shape consistent with the measured,or the 20 percent measured power shape annealing matrix. That was a major problem. We fixed our ex-core shape on the predicted shape annealing matrix. When the shape annealing matrix did change, our power distribution calculated with the fixed ex-core shape was very conservative.

It had an ASI calculated on the order of minus .6, plus or minus .1. So it was a very conservative calculation.

We implemented a corrected ex-core shape.

The second change was we raised the breakpoint power. Previously the breakpoint power was about 1-2/3 percent linear power. Based on the ex-cores, the shape that we were provided with would be conervative up to power levels of about 15 percent. And we asked ourselves questions about signal or signal-to-noise ratios at low powers, and we decided to make the break point on the order of 5 percent power.

The third change we did to eliminate the chattering about the breakpoint was to add a hysteresis band, so that we would use a fixed ex-core shape for powers below 5 percent and the actual power shape for powers above 7 percent all the time, and in the range 5 to 7 percent it depended on which direction we approached the breakpoint.

(Slide.)

After we implemented this change, Arkansas had no problems with crossing this boundary point.

The second software change we implemented for the Arkansas Cycle 1 was we made modifications to the CPC and CEA position dead bands. In the early CPC design, we only had dead bands of 7-1/2 inches. Technical specifications require rod exercising every month, moving the rod five inches to assure that they will move. And the five inches, plus the uncertainties associated with CEA positions, could possibly cause spurious trips, channel trips or plant trips. So increase the dead band to 11 inches, or 7-1 percent.

In the CEAC, we had no --

MR. KERR: Excuse me. What is meant by increasing the dead band to 11 inches? In terms of indication or movement or something? What is it?

MR. ROZEK: In the previous design, in the top 5 percent of the core or top 7-1/2 inches of the core we permitted CEA deviations. The penalty factors were not applied. Our uncertainty analysis took into account small deviations in this upper 5 percent of the core.

This 5 percent, this is what I mean with the dead band. It inhibits the calculation of penalty factors for rod deviations within this 5 percent, because CEA exercising will require insertion of rods 5 percent, which is roughly 3-2/3 percent.

We increased the size or the magnitude of this dead band, so we would have a larger area without penalty.

MR. KERR: The dead band is now the upper 5 percent?

MR. ROZEK: The upper 7-1/2 percent.

MR. KERR: Thank you.

MR. ROZEK: In the CEAC, our original design did not have dead bands at all, which could possibly result in a reactor trip if, during the rod exercising, one of the operators inserted the rods too far by accident. So we increased the size or we added dead bands, with logic similar to the CPC logic, with a magnitude of 7-1/2 percent.

The third change we made we made modifications to the dynamic power calculations. The dynamic power thermal calculation is based on the rate of change of the hot leg temperature. This calculation was fairly sensitive to noise. We reduced the sensitivity to noise.

MR. LIPINSKI: Could you be more specific? What did you do, put a filter in?

MR. ROZEK: Okay. The filter that was in there, that represented this dynamic term, was a lead filter. It accommodated transport time delays and the RTD time delays associated with the increase of hot leg temperature. And the gain on this filter was 13 percent power per degree Fahrenheit, which was fairly substantial.

We went back and looked at this gain and reduced it.

MR. LIPINSKI: Wasn't that put in to try to compensate for the lag time and not the measurement?

MR. ROZEK: That is true. But we found we could compensate with a smaller gain.

MR. LIPINSKI: But you didn't effectively compensate for it. In effect, you took some of the lag of the measurement.

MR. ROZEK: Could you repeat your question?

MR. LIPINSKI: Wel' first of all, you had a measurement that had lag time in it. To try to offset the lag time, you put in a lead filter. Now you found out that it was noisy because it had a derivative characteristic to it. So you backed off on the differentiation.

And effectively, you have gone back and accepted more of the lag from the initial measurement.

MR. ROZEK: Can I illustrate this with you, the difference between the old filter and the new filter? And I hope I can satisfy your question.

MR. KERR: Well, if what Walt said is true, you don't need to illustrate it any more. He understood it. Does he understand what you meant or not?

MR. ROZEK: He has it half right.

(Laughter.)

MR. ROZEK: What we had essentially would be time and power. During a single CEA withdrawal event, the actual power would go up like this. The CPC-calculated thermal power would have a lag. It would go up like this, where this would be flux actual and this would be the CPC static thermal power uncompensated.

By order of design, the gain on the dynamic thermal power compensation ideally should bring the static thermal power equal to or greater than the actual power. The optimum compensation did this, but it brought it up like this. So we were optimized with this increasing power, but it jumped up and down. It was noisy as the power increased.

What we did was reduce the magnitude of these jumps, and then your design goes up sort of like this. So there is less sensitivity.

MR. LIPINSKI: If I recall, I think you took your simple first-order transient time constant and simply applied a first-order difference. Now you are illustrating, due to the fact that you have a sampling process, that you've got an oscillation. I think if you went back to the digital filtering theory, I think you could even get rid of those oscillations and make it acceptable.

MR. ROZEK: The form of the filter --

(Slide.)

MR. KERR: He was just trying to illustrate that he understood more than half of it.

(Laughter.)

MR. ROZEK: Okay. I'll accept that.

Based on the input sweep testing that Ed Brown brought up earlier about the small differences in input machines between the CDC 7600 and the Interdata-716, we found that our heat flux and local power density filters were susceptible to truncation at certain power levels.

The susceptibility began about 90 percent power for heat flux, which is where you don't want to have additional errors. This was due solely to differences in machine precision between the Interdata and the CDC 7600.

We represented our filters previously by a direct form, where the current value of the output depends on the current value of the input plus current values of the input, and on the current values or the past values of the outputs. What we did was, we transformed this filter from what we called the direct form, the way it was implemented, to a cascade form, which was less sensitive to truncation noise on the Interdata-716.

So the filters had the same response, but had less sensitivity to machine precision truncation.

MR. KERR: What do you understand of that, Walt? I understand about 20 percent of it.

MR. LIPINSKI: I'm willing to let that one pass, rather than stimulate a half-hour discussion.

MR. KERR: Go ahead. He understands it.

(Laughter.)

MR. ROZEK: The fifth change was we went to floating point arithmetic. Ed Brown mentioned this earlier. We made this change because the software is easier to maintain with this change, the software is more accurate. And in the previous design the CPC's would be in a continuous auto-restart mode, and would not be calculated as certain shutdown conditions with no pumps running, for instance, or three pumps running and shutdown rods inserted. It would be in this continuous auto-restart mode.

Changing to floating point arithmetic, we had the capability to have the CPC run performance calculations in shutdown conditions.

MR. LIPINSKI: How many digits are you carrying in terms of the digital accuracy? They've got bits. I don't know how they do their change to floating conversion.

MR. ROZEK: I will defer to Mark Stofko.

MR. STOFKO: Mark Stofko of CE.

The floating point arithmetic in the Interdata-716 computer has a 32-bit configuration. 24 bits represnt the mantissa and 8 bits for the exponent.

MR. LIPINSKI: Is that plus or minus, that exponent?

MR. STOFKO: There is an excess 64 notation. I don't know if you are familiar with that, but that would be plkus or minus.

MR. LIPINSKI: Plus or minus 8 bits? I'm trying to get a feeling as to whether I'm going to see a number that's 10,000 in terms of the mantissa part and 10 to the minus 99 to 10 to the plus 99 in terms of the exponent part.

MR. BROWN: Ed Brown, CE.

It's seven bits plus a sign bit. It's 10 to the minus 69th to 10 to the plus 69th.

MR. LIPINSKI: Thank you.

MR. ROZEK: The next change we made is changes to the CPC initialization. The CPC initialization was the change of one constant to permit the calculator to be run with less than four pumps running in shutdown conditions. The CEAC initialization was a change that we implemented, that Tom Cogburn brought up. It was the second design error in the CPC's.

MR. KERR: What's this, quote, "design error"?

MR. ROZEK: The, quote, "design error," I would say is the flaw.

MR. KERR: Okay, we'll accept flaw. Where we would say "error," it is translated into "flaw."

MR. ROZEK: The objective with the CEAC initialization was to eliminate the possibility of CEAC trip caused by an unnecessarily large penalty factor being generated after an auto restart. The CEAC auto restart would be generated after the testing, periodic testing of the CEAC, or after reload of the CEAC software.

In the previous design, a very large penalty was applied on the length of the CPC after initialization. If the CPC read this large penalty factor, it resulted in a trip. In seven cases for Arkansas, it did result in a trip.

What we did was, after the CEAC comes out of initialization, instead of having an extremely large -- or the largest penalty factor that could be transmitted, it transmits the realistic penalty factor.

(Slide.)

The changes I have just listed are the changes that were implemented as a part of the Mod 1/2A software package that was implemented in June of 1979. The following changes are the changes that were implemented at Arkansas in May of 1980 and are part of the Mod 2B/3 changes.

We have added the capability for the CPC's to provide reactor protection for certain asymmetric steam generator transients. In the original Arkansas design and the way it is licensed now is that protection for asymmetric steam generator transients is provided by the low steam generator level trip. This required a trip setpoint on the order of about 40 to 50 percent, am I correct, Tom?

Without having to provide protection for certain isometric steam generator transients, the setpoint could be lowered on the order of 10 to 20 percent. During Arkansas startup, when the feedwater controls were in the manual mode, there was a possibility for reactor trips to be generated because of not keeping the water level constant, and reactor trips did occur. I don't know how many.

What we did was make a modification to the CPC system to provide protection for single MSIV closure in the CPC's. This changed the base on looking at the cold leg temperatures during an asymmetric steam generator transient. The cold leg temperatures will diverge and account for sensor time delays, and essentially have put in a trip based on the difference of cold leg temperatures.

MR. KERR: Now, steam generator transient is a situation in which steam generators behave differently in turn?

MR. ROZEK: That is true.

MR. KERR: Right.

MR. ROZEK: We altered the design slightly so that we would have input for thermal filters, so that we would have input based on thermal power and flux power.

The next two changes I am going to discuss in a little more detail. They are the CEAC penalty factors and the CPC-CEAC diagnostics that we added.

(Slide.)

The objective with the penalty factor changes are to reduce the number of unnecessary CPC trips as a result of the CEA deviation logic. As was brought out earlier, the CPC's must provide protection for CEA deviation events. But all deviation events do not need to result in a trip. For

-4

example, rod drops at zero power, 10 percent power or full power, there is enough margin in the core not to have a reactor trip.

In the previous design, the CEAC calculated one worst-case penalty factor that was applied both to the DNBR calculation and the local power density calculation. This worst case penalty factor was independent of the CEA configuration. So therefore, the result of a dropped CEA with all rods out, the same penalty was applied in the CPC's as for a drop of a CEA with the rods heavily rodded. The penalty factor was applied to the one pin radial peak and the CEAC/RSPT, and our logic only permitted both CEA's to be in service or both CEAC's out of service.

This change was requested by AP&L for the following reasons: First, if there were spurious inputs to one of the CEA calculators on one CEA, it required turning off that CEA calculator. By turning off that CEA calculator, you lost information from the other CEA's, especially to the CRT display.

The only way to do it was physically turning off the computer. What they wanted was a capability to leave the computer running, but to inform the CPC's that the CEA calculator was calculating spurious penalty factors, and that essentially the plant is operating in the one out of one CEA logic permitted, or the CEAC mode permitted by tech spec.

The changes that we made are we now calculate separate penalty factors for DNBR and local power density. These penalty factors are based on the magnitude of the deviation, how large is the deviation of one rod compared to the other three rods in the core, the direction of the deviation, is the deviating CEA above all the other CEA's in the subgroup or below the CEA's in the subgroup.

This is as far as the dependency was in the original Arkansas design, so the following changes were added. Number C, we made the CEAC penalty factors dependent on the subgroup division, which subgroup had the deviated CEA.

We made the penalty factors based on the CEA deviation on which rods or which banks are inserted into the core. We also made the penalty factor dependent on time. We have added a dynamic xenon component. We increased the amount of information transmitted from the CPC -- from the CEAC to the CPC.

Previously, we transmitted a fail flag which informed whether the penalty factor was good or not good, and one penalty factor. We have continued to transmit this fail flag. We transmit both the DNBR and the local power density factors, and we also transmit a penalty factor flag which is essentially a trip flag, so that we can do our scaling on our 16-bit length with the most benefit.

We applied the penalty factor to the heat flux. The penalty factor on gain was based on power margin, and it was appropriate to apply it on the heat flux.

We modified the logic so that one CEAC could be left in service, the other CEAC, the CPC would know that CEAC could or was providing a spurious output, but the operator could use the CRT display to monitor the other 80 rods. And we modified the CEAC CRT display.

(Slide.)

The previous display was just a bar chart and that's all there was. The numbers that are on the left-hand and the right-hand side, and on the bottom and the top were decals that were pasted to the CRT. And if there was a horizontal problem with the rods, this underneath here did not correspond to the numbers if there was a slight shift.

(Slide.)

We modified the CRT display to get more human engineering into it, so that we would have the CEA positions in the groups and subgroups and individual CEA names provided on the screen, written by software. The first column up here indicates which regulating group or shutdown group the CEA's below it correspond to.

The second line is the subgroup number, subgroups 10 or 11 or in regulating group 1. And the next set of lines are the individual CEA's in these subgroups. So for these subgroups or regulating group 6, that is inserted; that is group 12; and CEA's 46 through 49 and CEA 1 are in this group.

If there was a failure of the CEAC sensor, the operator, if he did not know immediately which rod it was, he could go to the display and it would count over which rod had the sensor indication.

We also put on the display what the values of the penalty factors are, so that operators, if there is a deviation of rods, the operator will have an immediate indication, if he looks at a CRT, of what is that effect going to be on his power or on his DNBR margin or his local power density margin.

If he saw a penalty margin of a 5 percent penalty, he would know that deviation is relatively small and he should correct it. If he saw a very large penalty factor, he would require a quicker action.

The number in the corner here --

MR. KERR: The change to which you have been referring has been implemented only in ANO-2?

MR. ROZEK: Yes.

MR. KERR: And the operators tell you that they get a lot more information on this display than they previously got?

MR. COGBURN: Our operators are much more pleased with this display than the previous one. I believe it gives a substantial amount more information, and it is certainly much easier to decipher.

MR. ROZEK: The number in the upper right-hand corner corresponds to which CEAC is being looked at, either CEAC number 1 or CEAC number 2.

The square is a cycling block that turns on and off, to let the operator know that the CEA display is valid. If this block was not turning on and off, it would indicate that the CEAC had failed and the information here is no good.

(Slide.)

This slide is similar to the first one. You notice that the block is turned off and is cycling. It indicates deviations overall. The "P" indicates that there is a penalty being applied in the subgroup because of the deviation of the subgroup. The "A" indicates that there is an alarm condition. The deviation magnitude is sufficient enough to cause an alarm. It is not sufficient enough to cause a penalty factor.

The penalty factors are provided here.

The next change for Arkansas Cycle 1, the second modification was a CEA-CPC diagnostics --

MR. KERR: Excuse me, Mr. Rozek. How much longer is your presentation likely to take? I'm trying to judge as to whether I should take a break now.

MR. ROZEK: 20 minutes or 25 minutes.

MR. KERR: Would you feel hurt if we took a ten-minute break at this point?

MR. ROZEK: No, sir, I would not.

MR. KERR: Okay. I declare a ten-minute break.

(Recess.)

(Slide.)

The next area of discussion is the CPC-CEAC diagnostics that we added into the CPCs that were implemented at Arkansas in May of 1980. Our purpose was to provide additional diagnostics to identify the cause of spurious CPC trips.

The previous design we had status words in the CPC that would provide an indication that a sensor had failed. That's the only information we had that some time from the previous time it was looked at that a sensor had gone out of range.

The changes that we made in order to facilitate this diagnostic capability was we added fail sensor stacks in both the CPCs and the CEACs. These stacks store up to six entries. An entry is made when a sentry changes state and goes from in-range to out-of-range or out-of-range to in-range.

It contains an ID name which corresponds to the sensor so the operator will look at it and see sensor 7 and know it corresponds to a hot leg temperature. It contains a status, whether it has failed out-of-range low, out-of-range high, or is now currently opearable, and the time of the entry. This time is a relative time since the CPC or CEAC restart time.

This sensor stack can be assessed in one of two ways. The first way is through the operator's module. We have assigned 19 18-point IDs to look at these fail sensor stacks so the operators can punch in numbers and record numbers through the operator's module.

The second method is if the calculator is placed in test, a hard copy record can be obtained through teletype.

The second diagnostic change we implemented in the CPCs was to provide a snapshot in case the penalty factor was calculated by CEAC or the trip was calculated by a CPC channel. This snapshot we found to be useful for many trips due to spurious reasons that Arkansas CPC would trip. It's a very fast-responding system. It trips for some events within 600 milliseconds, and we have no indication why it tripped.

The snapshot stores in memory certain variables used in the CPCs -- the inputs, the addressable constants, certain intermittent variables like flow power, ASI, and the outputs to the DNBR that's being calculated.

As I said earlier, this buffer is filled in the CEAC if a off-normal penalty factor is generated. For CPC this buffer is filled if the buffer is tripped.

MR. RAY: What triggers the snapshot?

MR. ROZEK: In the CPC, a channel snapshot, if it calculates below that, it will take a snapshot of a certain data and store it there until the operator releases that.

In this sense there is a large amount of data recorded in a snapshot, about a hundred variables in point IDs and inputs in this date list. It is accessible only through a teletype when a calculator is placed into test.

Another change we made is we added logic to prevent spurious penalties as associated with RSPT-associated instrumentation anomalies. This was touched on a little bit earlier. If sensed rod position was 150 inches withdrawn and 100 milliseconds later it was sensed at zero inches withdrawn or was sensed grossly out of range, we would alarm this indication. We would have the CEAC or no penalty calculated for this instrumentation error due to RSPT anomaly, and it would provide time for the operator to take that CEAC out of service and be an effective one out of one mode or both CEACs inoperable mode in a boiler reactor trip.

(Slide.)

In addition, if there are other modifications made during cycle 1, these are relatively minor modifications. We changed the saturation trip logic following Three Mile Island. There were some questions of the saturated temperature. We said well, indirectly we have a trip based on saturated enthalpy, because enthalpy is used in the DNBR calculation.

In order to help assist operators, we are doing this calculation, saturated temperature versus primary pressure. We also made changes -- we input some of the major power distribution constants.

MR. KERR: Excuse me. I'm not quite sure what you did as a result of TMI-2. I heard your discussion, but what did you do?

MR. ROZEK: After TMI there was some questions, can the CPCs when the coolant is at saturated conditions -- we said yes, except these calculations are one in the enthalpy space instead of temperature space.

As a result of Three Mile Island, we are doing this calculation in temperature space where we calculate the saturation temperature and the actual maximum temperature to compare the two. The CPCs have a trip logic in it, except this logic before was based on enthalpy.

By calculating on temperature, the operators can go to CPCs and have an estimate of how far away from saturation they are in temperature units.

MR. KERR: If it's calculated in enthalpy, can you do this?

MR. ROZEK: They would have to go to steam tables and convert the enthalpy back to temperatures. So there are changes on this order of magnitude also for Arkansas.

MR. LIPINSKI: Is there an automatic trip, or is it only displayed information if he chooses to look at it?

MR. ROZEK: No. There is a CPC trip when the sensed temperature is at saturated conditions.

MR. LIPINSKI: Is that moot for an assigned function?

MR. ROZEK: No, it is not moot. It was to provide protection on specific volume and enthalpy, which are only valid in the subcooled region. If we got out of the subcooled region, these would be no good, and we wanted a trip.

MR. LIPINSKI: Okay.

(Slide.)

MR. ROZEK: The next set of changes are the SONGS-2 changes which will be an upgrade from this current cycle 1 design. These changes will be also implemented in Arkansas cycle 2 in the following areas: the DNBR calculation, addressable constants, power distribution calculation, diagnostics and plant specific data.

I don't have a slide on plant specific data, but I will explain it briefly here. Plant specific data is exactly what it says. It's the number of CEAs that will be added to the CPCs using 91 instead of 81 characteristics of the core -- the larger core, larger power level, higher flow rate in that area.

(Slide.)

The DNBR calculation, we wanted to base our static

DNBR and our updated DNBR calculations on the CE critical heat flux calculation.

MR. KERR: Could you tell me in a few words why you wanted to do that?

MR. ROZEK: I'll defer to Bill Gill.

MR. GILL: Previous algorithms were an approximation to the W-3. That basically had the same information flow and the same functional form, where the CPC algorithm used approximations and curve fits to sum up the more complex iterations that would be in a design code like the W-3.

When we were fitting the CPC W-3 algorithm to the W-3 correlation, it fit very well and had low uncertainties. When the design basis algorithm for Southern Cal, the overall design plant basis correlation was converted to the CE-1, we now had a mismatch between the functional form and information flow to CPC in the design algorithm. We therefore went in and redesigned the CPC algorithm such that it was a better approximation, and therefore, uncertainty analysis would result in more uncertainty.

MR. KERR: I'm trying to understand what the operational results of that description is. Does that mean that you can get more power out of the same reactor?

MR. GILL: Yes.

MR. KERR: I was trying to search for -- to respond to what you said there.

MR. ROZEK: This slide essentially says what Bill said. The previous design was based on W-3 methodology, basing it on our CE-1 methodology, the CPC and the addressable constant area. We have implemented power distribution constants for CEA shadowing, radial peaking factor, and coolant temperature chattering which Tom Cogburn called temperature decalibration.

All of these changes were based on Arkansas cycle 1 startup experience. We found out that we could accommodate what was measured at Arkansas, but it resulted in increasing uncertainties that had to be applied all the time.

With adding certain addressable constants we can more accurately model the power distribution that CPC calculates as compared to the actual power distribution. We have made the DNBR and the local power density pre-trips at points addressable. In the previous design these were fixed numbers.

Our philosophy in this is that it is the utility's decision to decide where they want to have their alarm on these calculations. What we foresee is that they would be operating at a nominal condition and be, for example, calculating the DNBR of 1.8. They would set the set point at 1.7, so if they got off these nominal conditions, they would have an alarm, and the operator could take the appropriate action.

We have added a method for automated re-entry of addressable constants. We can write the addressable constants that we don't expect to change during the fuel cycle such as a startup-related addressable constant to a disc after a software reload. We can read these addressable constants back into the memory.

MR. LIPINSKI: Question. The addressable constants are entered from the console, and I believe they have a decimal point as part of their entry.

MR. ROZEK: They can. The floating point numbers will have a decimal point.

MR. LIPINSKI: Do you still have software validity checks as to whether the number entered is within the acceptable range?

MR. ROZEK: Yes.

MR. LIPINSKI: Did you have to change any of these from what you had already implemented?

MR. ROZEK: I don't recall any.

Did we, Bill?

MR. GILL: No.

(Slide.)

MR. ROZEK: In the power distribution calculation was made a couple of changes. We changed some fixed numbers in the calculation data-based constants. These fixed numbers are specified in our functional specification. They were based on Arkansas cycle 1 optimization of the power distribution calculation, and we wanted to make it so we could add numbers based on the cycle in the plant, so several numbers have been changed on that data base constant.

MR. KERR: Give me a for example.

MR. ROZEK: For example, in the shape annealing matrix there were checks at the end of power, less than 3 percent, and that 3 percent was a fixed number. We would do a certain set of logic. That 3 percent number is now a constant that we can calculate on a plant specific basis.

MR. KERR: Okay. Thank you.

MR. ROZEK: The second change is we have added a density dependent correction to the radial peaking factor. In the previous design we used radial peaking factors with uncertainties that were table look-up values based on CEA configuration alone. We have a density correction now.

MR. KERR: Density of what?

MR. ROZEK: Density of the coolant.

MR. KERR: Thank you.

And the density is measured on a global scale or --

MR. ROZEK: We measure it based on the cold leg temperature density.

MR. KERR: Okay.

(Slide.)

MR. ROZEK: Since Arkansas cycle 1 had our first try, our first cut at diagnostics, I think we did a very good job. We did want to improve them based on our operating experience there.

One of the changes is we changed the CEAC snapshot buffer. Before, it would take a snapshot whenever there was a penalty factor and update it every five seconds. Right now, based on the Arkansas design and because of delays in applying penalty factors, our trips after penalty factors, if the penalty factor is not large enough to cause a reactor trip and a couple of seconds later it does cause a reactor trip, we don't get a true indication of the data in the snapshot buffer which causes the trip.

We have changed it so it models the CPC, and we will think it will work better. I think it was kind of confusing.

The fail sensor stack ID numbers, in general we tried to keep the fail sensor stack ID numbers the same as the point ID numbers. We also enter in the fail sensor stack different --

MR. KERR: Excuse me. I don't understand the difference between a sensor stack ID number and a point ID number.

MR. ROZEK: Okay. A point ID number is when we go to the operator's module on the CPC and we say display XYZ. XYZ is called the point ID number, a number that corresponds to a variable; and the number will be displayed along with the value of that variable.

The fail sensor number is a notation; that stack number is the number that we use in our fail sensor stack. If you recall from an earlier slide --

MR. KERR: I remember that.

MR. ROZEK: -- Recall whether a sensor failed high out-of-range, in range. And generally what we wanted in our original design was to have the fail sensor ID number be the same as the point ID number; so if point ID number 005 corresponded to cold leg temperature 1, we wanted a fail ID stack sensor number to be -- if they saw 005 here, they would have the reinforcement to know that.

In fail sensor stack we also record stuff that is not true se values. We compared the difference in the CEA deviatio penalty factors. If the difference in the penalty factors is larger than sum epsilon, it could be the result of an anomaly or a spurious penalty being calculated by on of the two calculators. For example, if one CEAC is calculated in a penalty factor of 2.5 and one is calculated in a penalty factor of 1.0, we would not expect that big a discrepancy. With a discrepancy that big we want to alarm it to the operator, have him go check it out.

And to store this stuff in the fail sensor stack we arbitrarily assigned it numbers. These numbers corresponded to point ID numbers, and when the operators went in and they saw these numbers, they went to the point ID table, and if it was the wrong indication, we changed the numbers to something unique that would not be in a point ID list.

The third change was a CEAC-CRT rewrite.

(Slide.)

In the CEA display that we developed, the only portion of the CRT that is rewritten periodically is the penalty factors here and here, and all this information below here, the rod positions. The numbers above it, the group and the subgroup and CEA number, is independent or should not or is not going to change over the cycle life. So once this is written following a restart, it is not rewritten again.

What we have done is added an addressable constant in the CEAC to rewrite the entire CEAC display, including these numbers up here. This was required because when one calculator was placed in the test, the screen would go blank at one time during this test procedure. The operators, wanting to see the rod positions, would switch to the other calculator, and this information would be missing during the switching procedure. So we wanted to have the capability for the operator to put this information on the top back on to the screen.

MR. LIPINSKI: Why are the two rows interchanged? Look at the left, 44 and then 42?

MR. ROZEK: Okay. This is the Channel A target rod, the Channel B target rod, the Channel target rod, and the Channel D target rod, all the way down. Why the core was -- that's the way it was wired.

The ex-core stack for Channel C is in front of rod 44.

MR. LIPINSKI: Those quadrants were progressive, weren't they -- A, B, C, D, -- as you went around the radius of the core?

MR. ROZEK: No.

MR. LIPINSKI: Okay. Then I don't see what the correlation is by presenting these rows to the operator if you are not giving him the geometric orientation.

MR. ROZEK: Okay. Presenting these rows as the purpose of -- for example, if this rod was deviating right here like in this case, if he did not know by immediately looking at it which rod was deviating, he could go to this display, counter over two rods, 46, 47, and then withdraw that one rod.

MR. LIPINSKI: I understand that, but if I give you an overhead view of the core and ask you to tell me where section A, B, C, D are, then he doesn't have this geometric overview here, so how do you correlate these rows?

MR. ROZEK: I'll defer this to Bill Gill.

MR. GILL: Bill Gill, Combustion Engineering.

There is a core mimic which is basically a picture of the core on the control board which shows the rod position relative to the core layout, the actual bundle that the rod is in. That's another device that is not driven by the CPC, but he does have correlation with respect to a rod number in a spatial location.

MR. LIPINSKI: But how do I correlate the way you write out your loads to the way the rod is positioned in the core?

MR. GILL: You go to this core mimic. You go to the core mimic, and you will see basically a map of the core, a bundle arrangement. You will see a number and location. You will see a detector with an A, B, C, D on it.

MR. LIPINSKI: Let's start from the beginning. I was told that those rows were A, B, C, D.

MR. ROZEK: Target rod for Channel A and Channel B.

MR. LIPINSKI: Now, where are Channels A, B, C, D with respect to this geometric plan?

MR. ROZEK: My guess -- and Tom can correct me if I'm wrong -- if the core is divided into quadrants like this, it would be A, B, D, and C, where the letters indicate where the ex-cores are arranged, and everyone from CEN and AP&L is agreeing with me. So that's the way it is wired up.

MR. LIPINSKI: That's a subject for presenting information to the operator.

MR. ROZEK: We made other minor modifications to the algorithm. These included logic for two CEA subgroups. SONGS is different than Arkansas because it has the subgroups with two CEAS in it. We had to put the logic into it. Also, CRT here, for Arkansas we rewrote it at a two-second interval. The rods were updated every two seconds. For SONGS it has more rods.

We went over all possible rod configurations that could be illustrated by the screen. We could not update it on a two-second period. We've increased it to a period no greater than three seconds.

Also, changes have been on this magnitude point ID table associated with the other changes.

That concludes my presentation unless you have some more questions.

MR. KERR: Mr. Lipinski?

MR. LIPINSKI: On one of these sheets there are a couple of reports that indicate where the changes were documented, and I think that was on -- yes, the static DNBR. Were all the other changes documented?

MR. ROZEK: They are also documented in CEN-135. All the changes, with exception to the automatic re-entry of addressable constants, are addressed in CEN-135. CEN-147 is a CPC functional spec and contains all the related CPC changes.

CEN-148 is a functional spec and contains all the CEA changes.

MR. LIPINSKI: So there are three reports issued since the ANO-2 review -- the 135, 147, and 148?

MR. ROZEK: These were reports issued for the SONGS docket. There is one more report, the data base document, which has also been issued.

MR. LIPINSKI: But I'm sure you issued the entire reports in this supplement. These are not complete, are they?

MR. ROZEK: CEN-147 is the complete specification. CEN-148 is the complete functional specification of the CEAC.

MR. LIPINSKI: Thank you.

MR. KERR: Are there other questions?

Thank you, Mr. Rozek.

I show CEN and their free design and test data is the next item.

MR. KENNEDY: Dr. Kerr, we essentially covered items 5 in Mr. Spinnell's presentation this morning where he covered the design of the test data, but I believe Mr. Spinnell would like to make a few closing remarks to summarize the essence of today's presentations. It should take no more than two or three minutes.

MR. KERR: Okay. Yes, at some point somebody was going to comment on some of Dr. Lipinski's questions in more detail. Was that Mr. Spinnell?

MR. KENNEDY: Which particular questions are you referring to?

MR. KERR: I didn't write them down, but I thought you were asking for some detailed information on test procedures.

MR. LIPINSKI: I was given a copy from their manual, and it's being reproduced right now.

MR. KERR: Oh, so you have the information you need?

MR. LIPINSKI: I will have it after the reproduction. It's about a quarter of an inch of paper.

MR. KERR: Okay.

Mr. Spinnell.

MR. SPINNELL: Dr. Kerr, what we have attempted today to do is to cover the following topics.

One, we have attempted to put in perspective and give an overview on the core protection calculator system and its relationship to the plant protection system.

Secondly, we attempted to highlight the similarities between the ANO-2 design and the San Onofre design hardware and software.

Thirdly, we provided an assessment of the ANO-2 experience from operational aspects of the computers.

Fourth, we have discussed in detail the orderly, structured process that we have laid out for implementing software changes and factoring in this experience. And of course with the software change procedure, the acronym CEN-39.

And next, we have provided a description of how we factored in that experience from ANO-2 into the San Onofre cycle 1 software.

And lastly, we have provided an overall status of the qualifications in testing efforts on the San Onofre software.

If there are no further questions from the committee or any of its consultants, we will turn the meeting over to the NRC.

MR. KERR: Are there questions by the subcommittee or the consultants?

Let me ask you, you have mentioned at various times your efforts to eliminate some large fraction of errors in software. In this and in consideration of the maintenance and other things, what formal or structured, or whatever the word is, attention have you given to decreasing possibility of human error?

MR. GILL: I was afraid the last question would be a tough one.

(Laughter.)

Probably the benefit that I see of reducing human error is that we have added to the design process a defined structure. That defined structure defines the flow of work from exception through to the final software, by having that definition defined repeatedly. And how we make these changes, we bring new engineers on board or engineers or lesser experience, we can direct them to a design procedure which is very structured; and I believe that reduces error.

The penalty for an error is also much higher, a human error, say the functional design up front where we have basically a process that takes three months to make one change. That's the calendar time to implement a software change. The penalty of getting to the end and finding out you had an human error up front is just very high, so there is some built-in mechanism of, I will say, just paying more attention to the review in the up front engineering prior to the design effort as opposed to -- we are looking up front to make sure the functional design is correct before implementing the software design.

MR. KERR: I think I can characterize this by saying you have tried to set up an orderly design process where a number of people are responsible for seeing that things get done correctly.

I don't know if there is a better way. I was just looking for whether you had been able to come up with something unique in structure that would make human error less likely in this error.

I don't know what the answer is that I'm looking for, but as I read the risk analysis, qualitative discussions of it, it seems to me there is a consensus that the equipment -- I'm not sure about the software -- but the equipment works rather well, and that in a sense if one is looking for ways to make risk less and reliability greater, the area for concentration may be on human error.

And I just wondered if Combustion had any formal program which was aimed at what I see at least as a very important problem in however one wants to describe the risk and reliability.

Now, you've talked some about the design process. What about operation and maintenance? Have you or ANO-2 given any serious attention to a formal way of trying to decrease human error as it might enter this part of the process?

MR. BROWN: Ed Brown, CE.

We have been endeavoring to increase all areas of reliability system with respect to the human interaction. It's gone from an informal process to a much more formal process of the last three years as we have done generic research in human engineering.

A couple of areas I will highlight that we have looked into, number one, the operators' interface with the system. We have looked at the two basic elements of the operators' interface, the operators' module, and the CEA display and talked to the operational people to get their feelings and their experience, and I have also looked at possible errors and problems that have occurred in the field. And as you have seen today, we have endeavored to correct those problems.

The second area of operational concern is in the maintenance and testing area. We are endeavoring to include that interface so that the technician maintenance person can more easily diagnose a system problem. That area is also undergoing intensive review, and hopefully future corrections. So we have concentrated basically on three aspects -- the operational aspect, the design aspect, and the maintenance aspect.

MR. KERR: Well, let me pick maintenance particularly and ask a question or so. As you tried to decrease the probability of error there have you concluded that one is most successful by -- let me just throw out some possible ways -- better trained maintenance people, better procedures, simpler systems?

Is there any one thing that you have concluded that is an area of greatest payoff?

MR. BROWN: Right now I think all of the areas are equally important, with the status of the first system in Arkansas cycle 1 probably the area of greatest efficiency within the comprehensibility of diagnostics. In other words, the system was structured with systems, with things like error codes where a technician would have go to a manual and look up to see what that error code is; and we're trying to improve that by putting it in normal English language.

So it's a combination of better procedures which rely on better technical manuals and also better systems use. It's a combination of the three, so the human being can better read the information and has a better indication of the system.

MR. KERR: Thank you.

MR. COGBURN: This is Tom Cogburn again. I would like to add something to that.

Speaking in a general sense regarding training and procedures and speaking for Arkansas Power and Light and the way we approach this problem, we are placing considerable amount of more emphasis from a management point of view, from a money point of view, and a personnel point of view to people-type training.

Our training staff at the site has gone from approximately four individuals two years ago to about 15 now and is projected to reach about 45. These are instructor-type people.

Our training programs have gotten much more formalized in the last two years, and we are -- new personnel now don't even start a job until they have had about six months of training, and that is a totally new practice for our company.

I think the quickest payoff in making things more reliable is in the area of procedures, though, in making the procedures have a more structured approach and control mechanism. And in the CPC area with regard to operator use and maintenance technicians, this is the approach that we have had the most success in, making the procedures more detailed and more synthesized, and then relying on the human element a little less and still being able to take credit for the individual's ability to think and reason.

MR. KERR: Thank you.

Any other questions?

Let me ask CE if on the basis of experience at ANO-2 you are satisfied with your reliability of the CPC system. I don't mean that you think it has reached the end product, but you have some expectations of reliability.

Have there been surprises, or do you feel it's about as reliable as it needs to be, or where do you see this and perhaps subsequent computer-based information systems?

MR. GILL: I'd like to answer your question in two parts. One is our satisfaction with the performance of the system, and then I would like to turn it over to Ed Brown to discuss our satisfaction with the hardware in terms of specific reliability; that is, the reliability of the specific hardware we have in the plant.

With respect to the performance of the system, looking at it on a global scale, we were happy with the performance. It was the first of a kind system. It was a major step for CE to implement digital technology, and realizing that we would be first and have a lot of visibility, we had to assure ourselves that there would not be major faults such as unsafe failures in the system that would have a major impact on a setback in terms of putting digtal computers into vital functions in a power plant.

Our reasons for this are many-fold. The more obvious ones are we are implementing a basically complete digital control room. In our TVA Yellow Creek plant this is our system. That plant relies on about 18 processors to handle the overall control, both from control systems to operating to monitoring systems to protection systems. That is our advanced patrol system using the color-graphic CRT display system. So we were concerned about the future of putting computers in the plant, and that has significant impact on the conservatism that we put into the initial system.

Although on a global basis we are content or happy with the performance, we actually cannot be very happy with the large number of trips that have occurred at the Arkansas plant. We have kept our key people working full-time since criticality to make the software changes, monitor the performance, and assure that we correct any deficiencies in the plant such as performance and availability of that system will exceed the analog system in the power plants today.

We don't believe we're there yet. We believe we're 90 percent of the way there. With additional data from Southern Cal operation and official monitoring, about one year to two years on the Arkansas plant, we think we will be there.

In retrospect there is probably one area that was the most difficult decision for us to make as designers, and that was the safety grade rod drop protection. Putting a one out of two system, a one out of two protection system in a plant is obviously very risky. That's a system where a single failure can cause the plant to trip. We procrastinated a long time over that decision and looked at the tradeoffs between relying on operator reaction or control systems such as turbine run-back or other non-safety grade control systems, and looked at what we thought the risk in fuel failure would be based on history, and felt that that risk was unacceptable.

At that time there was a decision made. It was basically a safety performance decision as to whether we were willing to sacrifice power capability and/or spurious trips to have a higher degree of confidence to protect the plant from rod-related events

We made a decision to put in a one out of two protection system. We are still evaluating the performance and the wisdom of that decision.

We believe within the next year or so we will be able to reduce the one out of two trips, but it is not obvious we will achieve that goal. If not, we will have to look at alternatives, and I won't speculate here on what those alternatives are.

I can point out that we are not the only vendor that had to approach that problem. Other designers have also, and they have looked more toward analytical methods -- approved analytical methods, basically to show that their margin is in the core.

They have also looked at higher reliability control systems, and we have discussed briefly this morning the problems of relying on controls systems and the criteria applied to control systems.

The decision on the one out of two system was a complex one. It's one we're still evaluating, and it's one we're still working to make viable in a nuclear power plant. Whether we can proceed to four-channel CEA monitoring or some other means to make that safety grade protection more viable is still a question we have to pursue.

With respect to future goals we think the CPC has encouraged us to continue with the application of digital computers to power plants. We are in the process of extensive backfits to computers to our operating plants. These are to address things like NUREG-0696, safety display systems, where we are relying on computer design to our CPC system, so we are moving as a company full speed ahead.

We are cautious. We have learned some things from maybe moving too quick on Arkansas, but overall we think the experience was good, and we are content with the system. The hardware reliability is something that I will turn over to Ed Brown who can comment on our competence there and where we are headed.

MR. BROWN: Ed Brown, CE.

As Mr. Cogburn said, we believe the hardware system at Arkansas has adequate reliability. However, the designers are not satisfied with its current performance. In fact, Mr. Cogburn's goal of three times better is what I would consider a little on the low side. We would like to see it about an order of magnitude better.

MR. KERR: I was hoping you would say that, but I couldn't coax him to do that.

MR. BROWN: Well, Mr. Cogburn is a very cautious person.

(Laughter.)

MR. BROWN: We have constantly evaluated the Arkansas performance, and we will work with Arkansas and Southern California to continually improve the system. We have taken lessons learned from the Arkansas performance and factored that into the manufacturing of our second generation reactor protection systems, the first of which will be our Palo Verde system, our System 80 plant.

The areas of improvement that we make there are the data links, which in the earlier plants are 16-bit rod data links. We have changed to complete data links, so there are now no electrical connections between channels. This gives better isolation, better noise immunity, better performance.

In the area of the input-output system, we have gone to a much higher performance, much higher reliability system that will cure many of the problems that Mr. Cogburn talked about today. It has a much higher temperature specification and is much more rugged seismically and environmentally.

The computer system itself is essentially functionally the same, but is a later generation that is completely software-compatible. So the software developed for Arkansas would run on this other system.

The hardware in total is form-fit and function compatible with the Arkansas, Southern California Edison hardware.

MR. KERR: Thank you, Mr. Brown.

In discussions this morning, my memory is that Mr. Cogburn said that the hardware in ANO-2 was significantly sensitive to a 5 to 10 degree change in temperature. I think -- I don't want to misquote you -- I mean, 10 to 20. I wrote down 5 to 10.

But is that what could be expected when you designed the system?

MR. BROWN: We would expect to see some small reliability degradation of those changes. We would expect to see -- well, to give you an order of magnitude, when we calculated the reliability of the system, we calculated 70 degrees Fahrenheit plus or minus 10 degrees.

The normal operating temperature is 70 degrees. At 120 degrees Fahrenheit, which is the maximum operating temperature of the module, we would expect to see about a factor of 10 degradation in reliability, which is what the military has experienced.

MR. KERR: When you say 70 plus or minus 10, you would expect the system would perform anywhere within 60 to 80 degrees according to design specs?

MR. BROWN: That's correct.

MR. KERR: I don't want to get you into an argument here that you'd rather not get involved in. That was not the impression I got from your discussion. I don't want to make a big thing about this, but it seems to me you are making this fairly sensitive to the air conditioning system. And I'm not opposed to that, but the air conditioning system now becomes a very important part of this reactor protection system, it would seem to me.

MR. BROWN: Let me categorize it as far as the other process instrumentation in the reactor protection system. The CPC system in Arkansas is no more sensitive toward room temperature than the reactor protection system, the process instrumentation or the electronic control systems in that plant. They are all built to about the same type of standards and specifications, and utilize the same devices.

So their susceptibility to room air conditioning. that is about the same. The physical isolation of the CPC's in Arkansas 1 room to the closed ventilation system would cause a differential between the performance of the CPC system, the performance of the balancing process.

MR. LIPINSKI: Due to the fact it is isolated, you then have a source for common mode failure. And what are your technical specifications with respect to being able to continue operation if that room isn't cool?

MR. COGBURN: Well, with regard to technical specifications on room temperature, there are none.

MR. LIPINSKI: We now have plant protection [illegible]ent that is sensitive to its particular environment, and since it is in an enclosure you have only one air conditioner, now, I presume, in this air conditioner, that is unreliable.

MR. COGBURN: Well, the system has been proven to fail safe, and the failures in the air conditioning, inadequacies, cause failures in a safe direction.

MR. LIPINSKI: Don't count on that, because the only ones you have experienced to date have been safe failures. But if you let that temperature go to a high excursion, you couldn't convince me that you're not going to have two channels fail unsafe.

MR. COGBURN: I'm not going to try to argue with you about that.

I'd like to try to go back to the 10-20 degree variations. What occurs with the air conditioning system we have at ANO is that when the emergency cooling units are used, because their capacity is so large -- we see the temperature has risen considerably, and then they are turned on and it cools it down very rapidly.

Then we have got to shut them off. And the temperature control is cyclic. So there is a tendency to, in that mechanism, that controlling mechanism, for temperature -- to cycle temperatures up and down, and this seems to generate some failures.

In my estimation, they are probably in the data link time unit, and I don't really think that is probably a design consideration to cycle temperature over that range frequently. That is a problem that Arkansas Power & Light needs to resolve.

MR. KERR: There again, we probably discussed this, but it seems to me that the system is temperature sensitive, in whatever way, both in terms of operation or possible increase in failure rate. Everybody involved ought to realize this, and this becomes a fairly important part of the way in which it operates, because performance characteristics, if they depend on temperature and depend on temperature -- that is just about as important as anything else.

And I would -- I mean, I don't know whether it's too sensitive to temperature or not. But if one reads the LER's, there clearly are situations in which the LER was attributed to that, and I assume correctly.

MR. COGBURN: Well, I'm not sure that those LER's -- sometimes they contain some speculation. I hope that they make it clear that it is speculation when it is. The --

MR. KERR: I always believe what I read in official documents, especially LER's.

MR. COGBURN: My recollection of those LER's is that the words were something like "high room temperature is suspected" or something like that.

One point I meant to bring up while I was discussing the operating experience, I would like to bring up now, and this is reminding me of it, is the fact that the failures have been -- the concentration of failures is significantly higher in channels B and C, and this is another piece of evidence that points to temperature problems, because those channels are more heavily moded. They contain the CEAC hardware in those channels.

Another point is that measuring room temperature does not necesarily reflect a change in cabinet inside temperature. And we have not thoroughly instrumented those cabinets to determine what the temperature is. This is something we're considering doing, to try to -- I think we probably need to do, to make a more intelligent evaluation.

One other further item that is planned for the refueling outage beginning next month is to remove the in-core detector amplifiers from those cabinets. Each CPC cabinet has an amplifier in it. We are removing those, and that is a significant heat mode being removed from the cabinets.

It also should help the air flow distribution in the cabinets, and I believe that is going to help some.

MR. KERR: Thank you, Mr. Cogburn.

MR. LIPINSKI: I would like my memory refreshed. But when the system was originally under development, I recall that the cabinets were under full load and thermocouple measurements were made in the interior to find where the local hot spots were with respect to the solid state equipment. And from that you had concluded what your inlet air temperatures were and what you could tolerate, is that correct?

MR. COGBURN: That's correct.

MR. LIPINSKI: So given that you could maintain your air inlet temperature, based on your earlier work, you would not expect to see equipment failures. Are we seeing something different from what you experienced from your initial tests?

MR. BROWN: The initial tests were based on steady state values. They didn't include the cyclic nature of ramping the temperature back and forth, which would tend to aggravate problems and cause thermal shock on the integrated circuits and things of that nature.

If I may --

MR. COGBURN: We also modified the air conditioning.

MR. KERR: Mr. Brown?

MR. BROWN: One comment toward Mr. Lipinski's comment about the nature of the fail-safe system. We have analyzed the system and its analog and digital counterparts, and we believe the digital system is much more likely to fail safe in an adverse environment than an analog system, for the following reasons:

It has a minimum number of analog components that are monitored by the system itself. The basic structure of the system from there on out is dynamic, two-state and digital in nature. As temperature either goes up or down, the device will not change state when it shouldn't. And there are extensive diagnostics to pick this up and to cause the system -- force the system into the trip state.

Because of this, the system does have a very great tendency to fail safe in an analog nature. However, of the same nature, it would drift, and the amplifiers can drift in either direction, depending on whether they are inverting or not, in the analog-type calculator.

I would believe that a digital calculator, compared to an analog calculator in the same environment, would tend to fail safe probably 99 percent of the time.

MR. KERR: Are you convinced, Mr. Lipinski?

MR. LIPINSKI: I'm dwelling on that. It depends on how many bits fail and at what time interval, in terms of the discrete components that are in that system.

MR. KERR: Are there other comments or questions?

(No response.)

MR. KERR: Well, thank you for your comments. I think I certainly found them interesting and helpful.

I guess we have -- one thing I did not ask is whether you felt that the NRC review had been thorough and adequate. Have they reviewed what you have done appropriately? Maybe you should think about that a while.

MR. GILL: No comment.

MR. KERR: Because we are now going to hear from the NRC on the status of the San Onofre review. And Mr. Bill Morris I believe is the chief spokesman today. Mr. Morris?

MR. MORRIS: The primary basis for our review has been the previous acceptance of the CPC design at ANO-2, the adoption by San Onofre of the 27 ANO-2 positions expressed in the SER, the evaluation of differences between that design, especially of the software changes that have been covered by the previous reviews, audits of the verification and validation program, the review of operating experience, and the reviews and audits of the test program, which is what we consider to be closely related to the verification and validation program.

(Slide.)

As I say, with regard to hardware, we have not made a re-review of the system because of the similarity in the design. There are only a few changes, as described by the previous reviewer, of the executive software, and that is now under review for San Onofre.

When previous changes to the software have been made for ANO-2, we have reviewed that as necessary.

With regard to preoperational tests, we anticipate that the test proram for SONGS is adequate based on similarity of the previous ANO-2 test program. We intend to check that program after it is completed.

This program is closely related, as I said, to the software verification and validation program. We will audit the implementation of the VNB program for San Onofre to confirm that it continues to be an acceptable process.

We have under review the operating experience that has been discussed somewhat today, and we will continue to look at that with regard to environmental effects, the frequency of this, the sensitivity of the power supply problems. And we will, if it is necessary, reflect this review in what we do with regard to the tech specs as they reflect the maintenance and surveillance programs for SONGS.

Essentially, we are looking to confirm the previous judgments made from the specification review on the basis of what we see in the operating experience. If it is obvious that some changes between SONGS and ANO-2 are required because of this experience, that would of course impact the ANO-2 tech specs, because we are, again, looking at similarities between the two systems.

One of the areas of dispute has been the link between the CPC and the plant computer. That is position 20 of the ANO-2 SER. No review of this issue is now planned by the NRC.

We have based our review up to now and our conclusions up to now on the commitment by San Onofre to the 27 positions expressed in the ANO-2 SER. If, as we have been told today, there is no longer such a commitment, that may perhaps have some impact on this issue.

However, at this time we expect all 27 positions to be adhered to, including position 20.

Perhaps the major part of our review centers around the new algorithms and input data that will be made to incorporate the new thermohydraulics correlations and the new physics correlation. And you have heard, I believe, the explanation of what those changes are like.

Larry Phillips is going to continue with our presentation by going into that in some more detail.

I believe that there were some questions that we were expected to answer. They are on the second page of the agenda, I believe.

Question number one is: What has been the experience of the use of the data link between the CPC and the plant computer, and how would the NRC relate this experience to the NRC's current position on the use of this device?

The answer is that this is not an active area of review. In addition, I would say that the submittal made by ANO-2 to justify the expanded use of the data link does not necessarily contain the operating experience that we think would be relevant to the questions that were raised originally about the plant computer-CPC data link.

MR. LIPINSKI: Let me raise a question on the data link. We heard that in the case of Arkansas they had asked for you to rescind your position 20. They are kind of pleasantly silent.

What bothers me about no feedback is, did you receive the letter?

MR. MORRIS: We received a letter that essentially said, we would like to use the data link. Normally when we receive a request such as that, Licensee's silence typically indicates that we are either reviewing or we will eventually get around to the review and we will consider it at some later date.

But it has hardly ever been considered to mean that one can go ahead and make the connection and use the data link. The answer to the question is we do not have that as an active item under review.

MR. LIPINSKI: You do not?

MR. MORRIS: We do not.

MR. LIPINSKI: So effectively you concurred with it?

MR. MORRIS: No. That's the Licensee's assumption. That is not the assumption of the staff. It never has been.

MR. LIPINSKI: Is it on your list of futures?

MR. MORRIS: I believe it is in the hopper somewhere. But in the current situation it is not a very high priority item.

MR. LIPINSKI: But how does this go with position

20, where they had 10 days to use it and they were told to disconnect it? They did not disconnect it, according to --

MR. MORRIS: We only learned of it today. Quite frankly, I think we were all surprised.

MR. KERR: Mr. Morris, I'm a little puzzled by that, because I read a letter in September which indicated that the data link was -- addressed to the NRC, so I assumed that it got somewhere -- that's the way I got it. It indicated that the data link was connected and they wanted to keep it connected.

It therefore comes as a surprise to me that this is a surprise to you, unless you --

MR. MORRIS: I think we interpreted the letter to say that, we are now using it -- we may want to go back, knowing what we now know, and look at the wording in that letter carefully. During the day I haven't had a chance to look at it, but I think I interpreted the letter to mean that they requested the expanded use, and I did not interpret it to mean that they had adopted --

MR. KERR: I've read the letter and it doesn't say anything about expanded use that I know of. But I guess it would be a good idea for you to read it.

MR. MORRIS: Well, I would prefer not to go into this in great detail now. I think it is probably for the

Office of Inspection and Enforcement to probably address this issue.

MR. KERR: Okay. Then your question about the use of the data link is that NRC really does not have much information on the experience with the data link, and you have not changed your position; is that your response?

MR. MORRIS: Yes.

MR. LIPINSKI: How does that apply to San Onofre?

MR. MORRIS: We had assumed, as I said before, that San Onofre was adopting all 27 positions. Essentially, we were going to utilize to the maximum the previous work done on the acceptance of the ANO-2 design and the positions regarding the CPC's, and that included position 20, which was an explicit statement of how the data link was to be used.

And on that basis, we had gone on the assumption that San Onofre was not intending to use the data link in another way than they had proposed in position 20.

MR. LIPINSKI: As a system for startup and then not use it during operation?

MR. MORRIS: That's correct.

MR. EPLER: If I understand correctly, the data link stands guard over instrument drift that could be unacceptable. I don't think how we could be -- could support a position of taking off the data link without assuring ourselves that the operation would be safe.

MR. KERR: Mr. Epler, I have never supported removing the data link from the first day I heard of it.

MR. EPLER: Well, I would agree with that.

MR. KERR: I am unable to prevail.

MR. EPLER: I'm not supporting the use of the data link. I am simply saying I don't think we can operate without it.

(Laughter.)

MR. KERR: But the problem is that the NRC doesn't have this information. From what Mr. Morris said, they really don't have any information on the experience with the data link. And it seems to me that somebody has been remiss in information transmittal. Because it seems to me that if the experience has been favorable, that this should have somehow been transmitted to the Nuclear Regulatory Commission.

I would urge that whoever has this experience, let the NRC have it.

MR. EPLER: Are you leaving me with the problem because I raised the question, what is the experience? And the answer I think I got, we can't operate without it.

MR. KERR: But the NRC didn't know that until today.

MR. EPLER: But we know it now.

MR. KERR: Yes. Well, that takes care of question one.

Question two, is that -- well, you received a request in a letter and you haven't done anything about it, at least through today.

MR. MORRIS: That is correct.

MR. KERR: Okay, so that takes care of question two. And you have -- well, I'll let you comment on how you want to answer three and four.

MR. MORRIS: I think a quick survey of the elements of our review indicated to some extent how we treated SONGS as opposed to ANO-2. And maybe it would be best, if you have further questions, to look at those specific items.

MR. KERR: Well, my impression from what you said is that you really haven't done very much additional review, that you had depended on the review of ANO-2.

MR. MORRIS: And the intention is that we would look at the changes, the changes that were elaborated on today. We will look at the operating experience and make confirmatory audits of elements of the program, such as the testing and verification validation.

MR. KERR: But up to now you have not looked at the ANO-2 experience in reaching any conclusion?

MR. MORRIS: Not to the extent that we made a conclusion about it. We have made cursory surveys of the LER's, as you have.

MR. KERR: Will you be able to make any more definitive a statement by the time the full Committee discusses San Onofre?

MR. MORRIS: We will be looking at the issue. It will be under review continually.

MR. KERR: But you will not reach a conclusion by that time?

MR. MORRIS: What time is the meeting?

MR. KERR: I would expect that you would know that better than I, since the NRC is reviewing it.

MR. MORRIS: Sorry. I thought you meant the full Committee meeting.

MR. SAVIO: It's Thursday, March the 11th, the second week in March.

MR. MORRIS: We will have had an opportunity to look at the data at that time, but we may not be able to make a final conclusion.

MR. KERR: And that gets us to question 4, which has to do with the failure modes and effects analysis.

MR. MORRIS: We do not intend -- I think to answer the question, we do not intend to request the failure modes and effects analysis of the system. We believe the previous seven man-years of review of the system by the staff and the elaborate analysis that have been done and the verification and validation program constitute an acceptable basis without a further analysis.

MR. KERR: Are you convinced that all the failures that might occur in the CPC would be fail-safe type failures?

MR. MORRIS: Yes.

MR. KERR: Okay. I have no further questions on those four questions.

Mr. Lipinski?

MR. LIPINSKI: In the earlier presentation, reference was made to NRC Question 221.18, which dealt with the software change. Could you amplify on what that question was?

MR. MORRIS: We have recently received a summary.

VOICE: I am addressing that completely in the first slide.

MR. LIPINSKI: Okay.

The other general question is, based on the experience to date is NRC considering a reg guide, a regulatory guide?

MR. MORRIS: We have plans --

MR. KERR: Excuse me. A regulatory guide on what, Walt?

MR. LIPINSKI: On the application of digital systems, because there are some do's and don't's that I think we could come up with.

MR. MORRIS: The answer is, yes, we are beginning some work on the guide. There is an ANSI standard, an IEEE standard out now. I don't know just what its status is at this stage. And we've looked at that and we have commented on that, and we intend to enhance that somewhat with our own experience from the ANO-2 reviews and other digital-based computer systems that we have executed for B&W and Westinghouse.

MR. KERR: Mr. Morris, on this -- that's one of your slides, or is this Mr. Phillips'? Okay, I'll ask Mr. Phillips.

MR. MORRIS: As I said, the algorithms and input data Larry is going to address.

MR. KERR: Mr. Phillips, would you feel hurt if I took about a five-minute break before your presentation?

MR. PHILLIPS: Not at all.

MR. KERR: Let's take five minutes.

(Recess.)

MR. KERR: Mr. Phillips, it's all yours.

MR. PHILLIPS: All right. I'm Larry Phillips, Core Performance Branch.

In our thermohydraulics review of San Onofre, we noted that the design basis for the thermohydraulic algorithms in the DNB correlation were being changed, and the CPC's.

(Slide.)

We felt that this was more than a trivial change and requested the information tabulated here, and the question 221.18, I believe was the number. On May 23rd, 1980, we asked for identification of revisions to the software specs for the CPC and the CEAC, which had been provided for ANO-2 and reviewed thoroughly there.

We asked for a test report on the San Onofre software when completed. We asked what modifications would be required to the ANO-2 base technical specifications as relate to the CPC's. We asked for a commitment from San Onofre to use the ANO-2-approved software change procedure, CEN-39, to accomplish all the modifications to the ANO-2 software; and for a commitment for them to obtain an independent review of software changes by a qualified consultant, and to provide documentation of the final software design.

After some -- oh, incidentally, in their initial response to those questions they indicated that the tech spec impact would be addressed later during the normal review of the tech specs. Actually, they indicated there would be no impact expected, but I don't see how that is possible.

They also gave the commitment to get an independent review from a qualified consultant. And after some arm-wrestling and further interchange, it was agreed that the documentation described in my next slide would be provided to satisfy the rest of the requirements.

(Slide.)

MR. KERR: Excuse me, Mr. Phillips. What was the qualified consultant going to review, the method for changing software or the software change?

MR. PHILLIPS: He was going to review not the method; they were going to use the methods of CEN-39. He was going to review the change in methodology and review the implementation in general, to just provide an independent review of the design change, to see that the design itself was accomplished correctly.

MR. KERR: The design of what?

MR. PHILLIPS: The design of the software change. In other words, the models provided in the functional specifications. That was our intent.

MR. KERR: So he was going to review the software?

MR. PHILLIPS: Yes.

MR. KERR: Now what is meant by "qualified consultant"?

MR. PHILLIPS: Well, a qualified consultant, I guess the classical definition is he lives so far away. But I believe there is a different -- probably a different interpretation in everybody's mind. We haven't asked --

MR. KERR: I'm not trying to get you on the record. I just wanted to know whether that term was different than a consultant.

(Laughter.)

MR. PHILLIPS: Well, I think when we say "qualified consultant," if the staff feels when they put that on it, if we were to ask of the qualifications of whoever was performing this independent review, if we felt they were inadequate, it would give us an opportunity to make that judgment.

MR. KERR: So you may ask them to tell you who they are going to give as a consultant beforehand, so you can pass on their qualifications?

MR. PHILLIPS: We may.

MR. KERR: But they don't know whether you're going to or not?

MR. PHILLIPS: Right.

MR. KERR: When are you going to tell them?

MR. PHILLIPS: Well, our review is actually just getting under way to a large extent. And if we're going to require one, I would say they would probably be told next month.

MR. KERR: Your review is just getting under way?

MR. PHILLIPS: Yes. Going to the next slide, I think you will see why.

MR. KERR: Okay.

MR. LIPINSKI: I would like to continue this discussion. Your consultant was for the software review; is that correct?

MR. PHILLIPS: For a review of the software design methods, methodology, and also, of course, looking at the test results and implementation as part of the judgment.

MR. LIPINSKI: But as I review this problem, I can take the CPC's as a black box and the problem is broader, because I have to go back to the basic considerations where some of these changes originated in terms of the functional requirements, and the original system is based on differential equations that got implemented by the software.

So your consultant's charter starts at what point? Where someone hands them different equations to install, not looking back at the very origin of why the change was made?

MR. PHILLIPS: Perhaps I'm being somewhat misleading in addressing what his charter is. I am addressing what seems to me to be the largest area of review in these changes. I wouldn't say it's limited to that.

Let me review the question as it was posed and the answer that was given exactly, and maybe you can draw your own conclusions from that. Quote: "To utilize the services of a qualified computer consultant to provide independent verification that approved changes in the software were properly made." Quote.

That was the commitment that was asked for.

MR. KERR: Approved changes, approved by whom?

MR. PHILLIPS: Approved by NRC.

MR. KERR: So in effect this consultant will also be reviewing NRC's approval.

MR. PHILLIPS: In effect, yes.

MR. KERR: So this won't occur until after you have approved --

MR. PHILLIPS: Well, "approved" would also be approved by the designer, by approval all the way around, actually.

And no, it does not have to wait on our review.

MR. KERR: Is somebody here from San Onofre?

MR. MOODY: Yes.

MR. KERR: Is it clear in your mind what you've committed to?

MR. MOODY: My name is Wes Moody. I'm the manager of nuclear licensing for Southern California Edison.

It's our interpretation of the staff's question

221.18 -- and this is the second part of the part identified by the staff as 5 -- that the staff is asking Edison to commit to retain, either as an outside consultant or an Edison employee, someone who is qualified to the same extent or to an extent similar to the requirement that's being placed on ANO in the tech specs to retain and put on the plant on-site review committee an engineer who is not only qualified in nuclear power plant engineering, but also qualified in software engineering.

And it's rather clearly identified in the Arkansas tech specs that he has that qualification.

MR. KERR: So if I had a copy of those tech specs I would understand. Is that in accordance with your understanding, Mr. Phillips?

MR. PHILLIPS: Yes. Let me read the sentence of their response which relates to it. Quote, it says: "SCE intends to utilize the services of a qualified consultant (may be an SCE employee) to independently review all software changes prior to implementation at San Onofre Units 2 and 3."

MR. KERR: Thank you.

MR. PHILLIPS: The documentation that was provided in response to our requirements was CEN-135, which was provided last September to the staff. It is a summary description of software modifications to the ANO-2 Cycle 1

CP software which is applicable to San Onofre.

The staff looked at that submittal, but did not conduct any in-depth review. We looked at it to the extent of understanding what was being done. But because of workload and priorities, we did not get into depth on it.

CEN-148, the CEAC functional design specs, was transmitted to us by letter dated January 19th. The CPC functional design specs was transmitted to us by letter dated January 21st. And the CPC and CEAC data base documents were received last week.

CE has promised a test plan -- or rather, the test plan will be asked for in ANO-2. But this would be a list of the tests which are planned in the final test, and that is basically due. And they will provide us the test results. We put March to May here. The latest we hear is that April is a good guess as to when that will come in. But those things have a habit of slipping.

So I guess basically, based on this and some things you are going to see in later slides, I would say that around SER time, which will be around the end of April, that the likelihood of our having completed this review and approved it is slim.

We expect that the license may very well carry a condition which is self-destructing upon completion of the review. We would see no problem with going to -- with not having approval prior to power operation.

MR. KERR: Let me see if I comprehended what I have heard. You said that the dates there when you got those documents through 149 -- and you say that the commitments have precluded any very extensive review of the documents so far.

Does the staff plan to review them?

MR. PHILLIPS: Yes, they are under review now. Of course, the 135 document is the only one that we have had for any significant length of time.

MR. KERR: No, I understand that.

Having reviewed them, is the staff planning to write an SER or a supplement to an SER? Or in what form will the staff's report on the review of those documents be?

MR. PHILLIPS: Yes, we expect that by April, SER time, that we will be able to provide substantial information concerning the progress of our review. And we will be able to indicate what is left to be done with the remaining work being done, in order for us to complete our review and approval.

MR. KERR: Okay. Thank you.

(Slide.)

MR. PHILLIPS: Some special considerations of the review, areas which interact, we feel, and could impact the schedule are: number one, there are a couple of items in the basic design review which are related. One is that San Onofre field has a modified grid spacer design, and we currently have under review the test data which indicates -- which is supposed to provide justification for use of the same DNBR limit value as being used -- as has been approved for the CE-1 correlation for standard fuel.

At the present time we have some problems with that. That limit value could change, of course. That would impact the software.

The next item is the method, which was changed rather late in the game. And this I think is just a matter of the mechanics of completing our review of the loss of flow calculation method. There are changes to the basic software, which are the large part of our review, and that would be the W-3, DNBR calculation, being replaced by CE-1, and the revision of the thermohydraulic methods.

And we have considerable questions on that, which we expect to get into with CE soon. The comparison we will want to see is a comparison of the CE methods to the approved design methods to assess the accuracy of the modified design.

(Slide.)

And, finally, the area to be reviewed is the power distribution calculation change changes which are reflected by these items, so that completes my presentation.

MR. KERR: Are there questions?

(Pause.)

In Supplement No. 1 to Appendix D, to what I believe to be a Safety Evaluation Report -- oh, this is ANO-2. There is language in the SER which says, after a certain preamble:

> "Therefore, we will require that the plant computer service data link to the protection computers be removed, and that the plant computer service routine be deleted, and automatic programs scheduled."

I guess later on you were more specific when they were supposed to be removed? Walt said something about 10 days.

MR. LIPINSKI: I believe that's what you have to conclude in their presentation.

MR. KERR: The ANO-2?

MR. LIPINSIKI: Yes.

MR. KERR: Mr. Cogburn?

MR. COGBURN: I have an excerpt in my hand from, I believe, Supplement 2 to the SER which says -- I'll read a paragraph from it:

"By letter dated" -- this is written, of course, by the NRC.

"By letter dated March 10, 1978, the Applicant agreed to use and operate the data links in accordance with our position; that is, all data links between protection computers and the plant computers will be connected during start-up and power system testing. Within 10 days after completion after the power system test, the six data links will be removed."

MR. KERR: That's where we got the 10 days. Now it would be helpful to me if I could -- I would have to make some sort of a report about this data, of the NRC Staff's review to Mr. Bender, and my apprehension is that there has been some additional review, but not much beyond ANO-2, but that you do now have these documents listed, that they will be reviewed, and that there perhaps will be some additional review of ANO-2 experience, and that this will appear in the SER. Help me with what I should tell Mr. Bender.

I think, yes, that we intend to look at the ANO-2 experience in determining -- in confirming or examining the adequacy of the tech spec maintenance and surveillance requirements.

MR. KERR: Okay. Now is it likely that that review, that part of the review, will be completed by what you referred to as SER time?

MR. PHILLIPS: April 30th?

MR. MORRIS: We intend to do that, yes. It is my estimation that the algorithms and data associated with the thermohydraulic correlations of the physics data is a much more extensive review than we will have to perform of the operating experience and the adequacy of the tech specs.

MR. KERR: Okay. Are there any further questions? Does that complete your presentation, Mr. Phillips?

MR. PHILLIPS: Yes.

MR. KERR: Does Staff have any further comment?

MR. MORRIS: With regard to the letter, I looked at it again, the letter from ANO-2 requesting the continued operation of the data links. I don't see any way we could have interpreted that to mean they intended to keep them in place, and that we, by being silent, would concur in that.

I wonder if Mr. Cogburn has any comment on that?

MR. COGBURN: I would prefer not to comment at this time. I think NRC and AP&L need to discuss this.

MR. KERR: I would think that's probably the case, too.

MR. PHILLIPS: I do have one additional comment that I think is related. Back from the original review, we had considerable difficulty in defining what changes are permissible without Staff review, or without being brought to the attention of the Staff, and we got language in finally which we felt went pretty far towards making this definition. A lot of the software changes -- or some of the software changes have been described to you this morning that have been accomplished in ANO-2.

There was a disagreement on whether these constituted reduction in margin and therefore an unreviewed safety question. So I think we -- as a matter of fact, we got some rather extensive changes. We were informed that they were being made or had been implemented, and the start-up was scheduled about three or four days later, or something like that, and we conducted a hasty review of those changes and got out some sort of a letter, I believe.

But there seems to be a continuing sort of problem as to what changes should be brought to the attention of the Staff and what can be performed by the operators without Staff review.

I believe that is kind of parallel to the data link situation.

MR. KERR: Thank you, Mr. Phillips.

Any further comments from the Staff?

My agenda shows comments by anybody who wants to make a comment at this point. Let me ask first if CE has any further comments.

MR. KENNEDY: No, we do not.

MR. KERR: How about Southern California Edison? Any further comments?

MR. MOODY: Yes, sir. Wes Moody.

From the standpoint of Southern California Edison, there are several items that I think are significant from today's discussion, and before I mention those two items, I want to clarify what I mean by from the standpoint of Southern California Edison.

We are right now delaying San Onofre Units 2 and 3 twice as a result of delays in licensing, and on the present schedule, we would have the units complete with construction some time this summer, which is substantially earlier than even the earliest date that would get the plant licensed.

The core protection calculators are one of just several remaining open items in the NRC Staff review of our application for an operating license, and so that's what I mean by from the standpoint of Southern California Edison, there is a couple of significant items here today.

The first item I wanted to mention was the fact that Tom Cogburn of AP&L has identified several issues whose significance has really become apparent as a result of the year and a half or so that they have operated with CPCs.

He indicated that they now recognize the significance of the controlling environment for the CPCS, and he also mentioned that they clearly recognize the advantage in the two out of three logic in the CPCs.

ar-7

We have the advantage for San Onofre Units 2 and 3 to design the plant around the CPCs, at least by comparison with Arizona -- excuse me, AP&L, and so both those elements have been factored into the design of San Onofre around the CPCs and, in fact, in case of the controlling environment, the CPCs are in the control room environment, and in the case of the logic, we have employed the two out of three logic.

The other item that --

MR. KERR: Is your control room environment better than Mr. Cogburn's CPC environment? The fact that it's in a control room environment doesn't mean much to me unless I know what the control room environment is.

MR. MOODY: At San Onofre we are able to put -- it's my understanding that Arkansas provided an environment for the CPCs after -- or midway in the plant design, perhaps even midway in plant construction, and as a result of that, had to provide a single separate room for the CPCs; whereas we are able to utilize -- we are able to incorporate in the design of the control room environment, including areas behind the panel, to house the CPCs as well as other safety-related items.

MR. KERR: That's all very well and good, but is the environment in the control room one that will take care of the CPCs?

MR. MOODY: We believe so, yes.

MR. KERR: It will keep the temperatures within the bounds that were discussed?

MR. MOODY: We believe so, yes.

The second point I wanted to mention was that both Tom Cogburn and Tom Rozek of Combustion Engineering identified software changes which have become important or of significance, have been realized as a result of the experience that AP&L has had for a year and a half, and those software changes are changes which are being reflected not only -- are reflected not only in the proposed changes for Cycle 2, for Arkansas, but also in the initial cycle for San Onofre.

So we and Arkansas are utilizing the results of the first cycle operation at Arkansas with our respective CPCs.

MR. KERR: Thank you.

Mr. Lipinski?

MR. LIPINSKI: When you say two out of three, ar9

it's basically a four-channel system; right? And you're calling it an installed spare, and only limited to two out of three by tech spec?

MR. MOODY: Al Spinnell can address that.

MR. SPINNELL: Mr. Lipinski, early on the review of the San Onofre document, we requested that the Staff conduct a review of the entire protection system on a two out of three basis, assuming that one channel of a particular trip function or any given trip function was out of service for whatever reason; maintenance, et cetera.

The Staff conducted that review not only of the protection system logic itself, but all of the balance-of-plant areas dealing with the power supplies from and including the station batteries through to the cabinets themselves, and the other interfaces that normally deal with the balance-of-plant scope.

The Staff, as I understand it, has written up in the SER in quite an amount of deal on Section 7 of the SER, details of the scope of that review, and their audit not only of the design documentation, but the walk-down of the separation of the four channels in that system, and we understand that they have confirmed that the operation of the plant protection system for San Onofre is acceptable on a two out of three basis, with one channel of a given trip function out of service a specified amount of time via the technical specifications.

MR. KERR: Mr. Ditto?

MR. DITTO: Do you still have only two CEACs? They are sort of asymmetrical, if you go to a two out of three system, instead of a two out of four.

MR. SPINNELI: That's correct.

MR. DITTO: Okay.

MR. KERR: Yes, sir?

MR. SRINIVASAN: My name is Srinivasan from the Staff.

I would like to clarify sort of a misconception that the protection system is an installed spare. You see this kind of learning in the FSAR. We, as the Staff technician -- there is a good reason in putting four channels to start with. What we did on San Onofre 2 and 3 was primarily to establish that there are really four independent channels. The Staff has completed its review and concluded that the design has really four different channels.

Now the Applicant, because of the Staff -- if he could operate the plant under some extraneous conditions where one of the channels is not operable, that becomes another issue, normally in the tech spec. We do not let a channel to be bypassed --- I mean not just bypassed, but tripped.

In this case, the Staff is willing to consider from only an external circumstance like the -- you may have a failure where you cannot fix it immediately unless you shut the reactor down, or there may not be an immediate replacement available.

For those cases, the Staff is willing to consider some external circumstances.

So I would like to correct the impression that the Staff is not considering to operate the plant on a three-channel basis. All four channels will be operable at all times.

MR. KERR: Is there a Staff requirement that all protection systems have to have four independent channels?

MR. SRINIVASAN: Well, if there is no requirement, there should be. But there have been some designs with four channel.

MR. KERR: If you have a three-channel, would you refuse to review it?

MR. SRINIVASAN: No, I wouldn't, personally speaking, I would not refuse to review it, because there would still be deliberations.

MR. LIPINSKI: Well, correct me if I am wrong, but you support IEEE 279. 279 allows one out of two and you allow bypassing of some reasonable amount of time to do maintenance on a single channel.

MR. SRINIVASAN: Yes, I do. As I said earlier, there are a lot of variances in having a four-channel system. Having got it, we don't want to give it up.

MR. KERR: But the merits of having a four-channel system disappear if you don't have it. If you require that people operate a four-channel system as if they have a three-channel system, it strikes me that you might have the fourth channel disappearing. I don't know, but if I were the Staff, I would give that some serious thought.

MR. SRINIVASAN: As I pointed out, we are not going to give up an accepted system. The plant will operate as a four-channel system.

MR. KERR: Yes, but suppose the next plant comes in and they say, "Those bastards over at the NRC won't give us any credit for having a four-channel system. Let's put in a three-channel system."

MR. SRINIVASAN: Well, somebody has to make a comparative assessment of what do you give up in giving up one of the channels.

MR. KERR: You don't give up anything, according to the single failure criterion, because you meet the single failure criterion with three channels, and that's all that the Staff currently requires, at least in the general design criteria.

If you start reading between the lines, maybe you'll find some other things. And I am simply asking that you not penalize people for going a little bit beyond the requirement.

MR. SRINIVASAN: That is exactly why we --

MR. KERR: I'm not discussing this issue, because I don't know the details, and maybe there is a very good reason that you want them to have four channels operating all at the same time. I don't know.

MR. LIPINSKI: Have you gone to a qualitative reliability requirement?

MR. SRINIVASAN: No. What do we gain and what do we lose by having three versus four, two versus three versus four.

MR. LIPINSKI: Improved reliability, for one. But unless you quantify it, you can't compare different systems.

MR. SRINIVASAN: We haven't done that exercise, I am sorry.

MR. KERR: Thank you for your comments.

Is SCE finished with its comments?

MR. MOODY: Yes.

MR. KERR: Does the representative of AP&L want to make any further comments?

T.15

MR. COGBURN: The point that I was trying to make regarding the four channels versus the three channels was mainly regarding the occurrences that are probably less -- I don't know what NRC's objective is in the licensee event reports system.

(Laughter.)

MR. KERR: Join the crowd.

MR. COGBURN: There is a wide disparity primarily in significant to very significant events reported in the system. There is a difference between a 14-day report and a 30-day report, but even within the 30-day reports, there is quite a bit of difference on one containment spray pump failing and being down. That is quite a bit more significant, I think, than having one CPC channel trip for a few seconds.

And this is the thing that I was really objecting to. We built the system to be, we thought, a three-channel system with an installed spare, and it was our intention to -- and then the tech specs were written such that any time we bypass a channel for any reason other than surveillance testing, it requires a writing of an LER, and I don't know that that is all that meaningful to have it done that way.

For instance, Arkansas Nuclear 1, Unit 1, is written -- the tech specs are written in the three-channel manner, and I think many plants -- probably all plants of that vintage are.

MR. KERR: Well, I think probably the representatives of the NRC who are here would agree with us, it would be nice if we could eliminate the trivial LERs from those that are important, and report only the important ones.

The problem is there is a "they" out there somewhere that continues to require LERs to be written about things that probably should not be written. Some day, that will be corrected.

MR. COGBURN: I hope so.

MR. KERR: I think safety will be enhanced, too, because I think some LERs are important and they ought to be looked at by everybody.

MR. COGBURN: Our reload licensing submittal for Unit 2 will include the proposed rewording of the tech specs to include that.

MR. KERR: Any further questions or comments?

Well, let me thank all of you. I must say that I hope that nothing that this subcommittee does or nothing that the Staff does will discourage people from trying to make improvements on reactor control and protection systems. Without trying to judge the merits of what has been accomplished by CE, it seems to me that it did take a certain amount of guts to probably -- the recognition of some of the things you would have to go through to work through the system, and it seems to me it could be an improvement, and I would hope that the industry continues, and I know that other people are doing the same sort of thing -- continue to try to improve things, even in the face of having to defend it before the ACRS.

(Laughter.)

Because it's only thereby that we are going to reach the goal of reliability that I think we would like to try to achieve.

So I hope that the questions and discussions are not interpreted as discouraging improvement or discouraging changes. I would hope that we don't do that.

Thank you again for your attendance and your contributions today.

Before I adjourn the meeting, I would like the consultants to give me any written comments that they consider appropriate within the next week or so, and we will be talking about the full committee meeting.

The meeting is adjourned.

(Whereupon, at 5:25 p.m., the meeting was adjourned.)

* * * *

end

NUCLEAR REGULATORY COMMISSION

This is to certify that the attached proceedings before the

____

in the matter of: ACRS/Subcommittee on Electrical Systems

Date of Proceeding: 2-24-81

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.

Mary C. Simons

Official Reporter (Typed)

Mary C Simons

Official Reporter (Signature)

NUCLEAR REGULATORY COMMISSION

This is to certify that the attached proceedings before the

____

in the matter of: ACRS/Subcommittee on Electrical Systems

Date of Proceeding: 2-24-81

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)

#1

CORE PROTECTION CALCULATOR SYSTEM (CPCS)

1. DESCRIPTION
2. COMPARISON OF SAN ONOFRE 2 AND 3 AND ANO-2 DESIGNS
3. DESIGN, QUALIFICATION AND FIELD STATUS
4. LICENSING STATUS

CRITERION NUMBER 10

(10CFR:50, APPENDIX A)

"THE REACTOR CORE AND ASSOCIATED COOLANT, CONTROL, AND PROTECTION SYSTEMS SHALL BE DESIGNED WITH APPROPRIATE MARGIN TO ASSURE THAT SPECIFIED ACCEPTABLE FUEL DESIGN LIMITS ARE NOT EXCEEDED DURING ANY CONDITION OF NORMAL OPERATION, INCLUDING THE EFFECTS OF ANTICIPATED OPERATIONAL OCCURRENCES."

SPECIFIED ACCEPTABLE FUEL DESIGN LIMITS

1. LHR

   CORRESPONDING TO CENTERLINE MELT

2. DNBR

   EQUAL TO 1.3 (W-3 CORRELATION)

CRITERION NUMBER 20
(10CFR50, APPENDIX A)

"THE PROTECTION SYSTEM SHALL BE DESIGNED 1) TO INITIATE AUTOMATICALLY THE OPERATION OF APPROPRIATE SYSTEMS INCLUDING THE REACTIVITY CONTROL SYSTEMS, TO ASSURE THAT SPECIFIED ACCEPTABLE FUEL DESIGN LIMITS ARE NOT EXCEEDED AS A RESULT OF ANTICIPATED OPERATIONAL OCCURRENCES AND 2) TO SENSE ACCIDENT CONDITIONS AND TO INITIATE THE OPERATION OF SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY."

CRITERION NUMBER 25
(10CFR50, APPENDIX A)

"THE PROTECTION SYSTEM SHALL BE DESIGNED TO ASSURE THAT SPECIFIED ACCEPTABLE FUEL DESIGN LIMITS ARE NOT EXCEEDED FOR SINGLE MALFUNCTION OF THE REACTIVITY CONTROL SYSTEMS, SUCH AS ACCIDENTIAL WITHDRAWAL (NOT EJECTION OR DROP-OUT) OF CONTROL RODS."

EVOLUTION OF LICENSING CRITERIA

NRC INTERPRETATION OF CRITERIA AND INDUSTRY KNOWLEDGE AND VIEWS IN REACTOR PROTECTION DEVELOPED AND CHANGED IN THE EARLY 1970's.

1. IN GENERAL SINGLE FAILURES OF AN ACTIVE COMPONENT SHOULD BE CONSIDERED AS A POSSIBLE INITIATING MECHANISM FOR AN AOO.

   ROD MISOPERATION EVENTS

   - SINGLE ROD WITHDRAWAL
   - OUT OF SEQUENCE INSERTION AND WITHDRAWAL

2. IN MOST CASES, OPERATOR ACTION SHOULD NOT BE RELIED UPON TO PREVENT THE SPECIFIED ACCEPTABLE FUEL DESIGN LIMITS FROM BEING EXCEEDED.

   - AXIAL FLUX PERTURBATIONS

BASED ON THESE CONSIDERATIONS AND THE POTENTIAL IMPACT OF THE RESTRICTIONS IN TERMS OF OPERATION, IT WAS CONCLUDED THAT THE PROTECTIVE SYSTEM MUST:

1. SENSE THE POWER DISTRIBUTION WITH INCREASED ACCURACY.

2. INCLUDE MEASURED CONTROL ROD POSITION AS INPUT.

3. PROVIDE INCREASED ACCURACY IN DNBR THERMAL MARGIN BY ON-LINE INTERPRETATION OF RELEVANT COOLANT SYSTEM PARAMETERS.

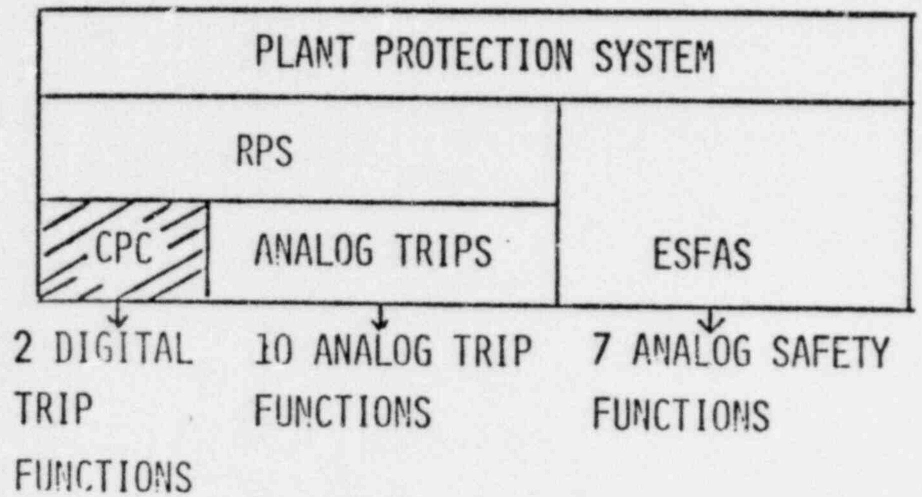
TO EFFECTIVELY IMPLEMENT THE ABOVE REQUIREMENTS, DIGITAL PROCESSING TECHNOLOGY WAS INCORPORATED INTO THE PPS.

THE SONGS PLANT PROTECTION SYSTEM (PPS) IS COMPOSED OF TWO SUBSYSTEMS:

1. AN ENGINEERED SAFETY FEATURES ACTUATION SYSTEM (ESFAS), AND

2. A REACTOR PROTECTION SYSTEM (RPS)

THE CORE PROTECTION CALCULATOR INITIATES TWO OF THE TWELVE TRIPS IN THE REACTOR PROTECTION SYSTEM, THE LOW DNBR TRIP AND THE HIGH LOCAL POWER DENSITY TRIP.



BACK-UP TRIP FUNCTIONS FOR CPC DESIGN BASIS EVENTS

FAILURE OF CPC WITH CONCURRENT AOO IS NOT A DESIGN BASIS EVENT FOR THE SONGS PLANT.

AN EVALUATION HAS BEEN PERFORMED TO DETERMINE BACK-UP TRIP FUNCTIONS.

RESULT:

EVENT	BACK-UP TRIP
UNCONTROLLED CEA WITHDRAWAL FROM A CRITICAL CONDITION	HIGH PRESSURIZER PRESSURE
UNCONTROLLED BORON DILUTION	HIGH PRESSURIZER PRESSURE
TOTAL AND PARTIAL LOSS OF REACTOR COOLANT FORCED FLOW	HIGH PRESSURIZER PRESSURE
EXCESS HEAT REMOVAL DUE TO SECONDARY SYSTEM MALFUNCTION	LOW STEAM GENERATOR WATER LEVEL
STEAM GENERATOR TUBE RUPTURE	LOW PRESSURIZER PRESSURE
CEA MISOPERATION	MANUAL TRIP

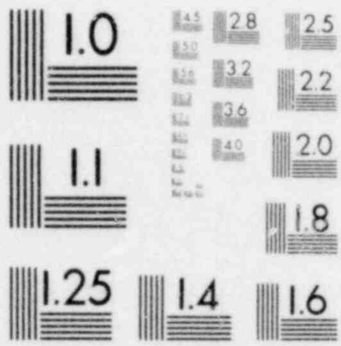
CPC SCOPE

1. SIGNALS FROM SENSORS THAT MONITOR SPECIFIED CORE VARIABLES
2. DEDICATED COMPUTERS (6) TO IMPLEMENT ALGORITHMS THAT WILL PROCESS THE SENSOR INFORMATION
3. OPERATORS MODULES
4. OUTPUTS FOR DISPLAYS, ALARMS AND REACTOR TRIPS

IMAGE EVALUATION
TEST TARGET (MT-3)

6″

IMAGE EVALUATION
TEST TARGET (MT-3)



6″

CPC

THE CORE PROTECTION CALCULATORS ARE DESIGNED TO PROVIDE THE FOLLOWING PROTECTIVE FUNCTIONS:

A. INITIATE AUTOMATIC PROTECTIVE ACTION SUCH THAT THE SPECIFIED FUEL DESIGN LIMITS ON DNBR AND LOCAL POWER DENSITY ARE NOT EXCEEDED DURING ANTICIPATED OPERATIONAL OCCURRENCES, AND

B. INITIATE AUTOMATIC PROTECTIVE ACTION DURING CERTAIN ACCIDENT CONDITIONS TO AID THE ENGIEERED SAFETY FEATURES SYSTEM IN LIMITING THE CONSEQUENCES OF THE ACCIDENTS.

CPC DESIGN FEATURES

- AN ON-LINE PROTECTION SYSTEM USING 3 LEVELS OF EX-CORE DETECTOR INFORMATION
- A COMPLETE SYSTEM OF DEDICATED DIGITAL CALCULATORS TO PROVIDE FOUR CHANNEL REDUNDANCY
- USES AN AXIAL/RADIAL SYNTHESIS TO CONSTRUCT POWER DISTRIBUTIONS
- USES MEASURED CEA POSITION INPUT
- FLOW DETERMINATION BASED ON RCP SPEED MEASUREMENTS
- LINEAR HEAT RATE AND DNBR CALCULATED ON-LINE
- OPERATOR'S CONSOLE PROVIDES COMPREHENSIVE DATA DISPLAY

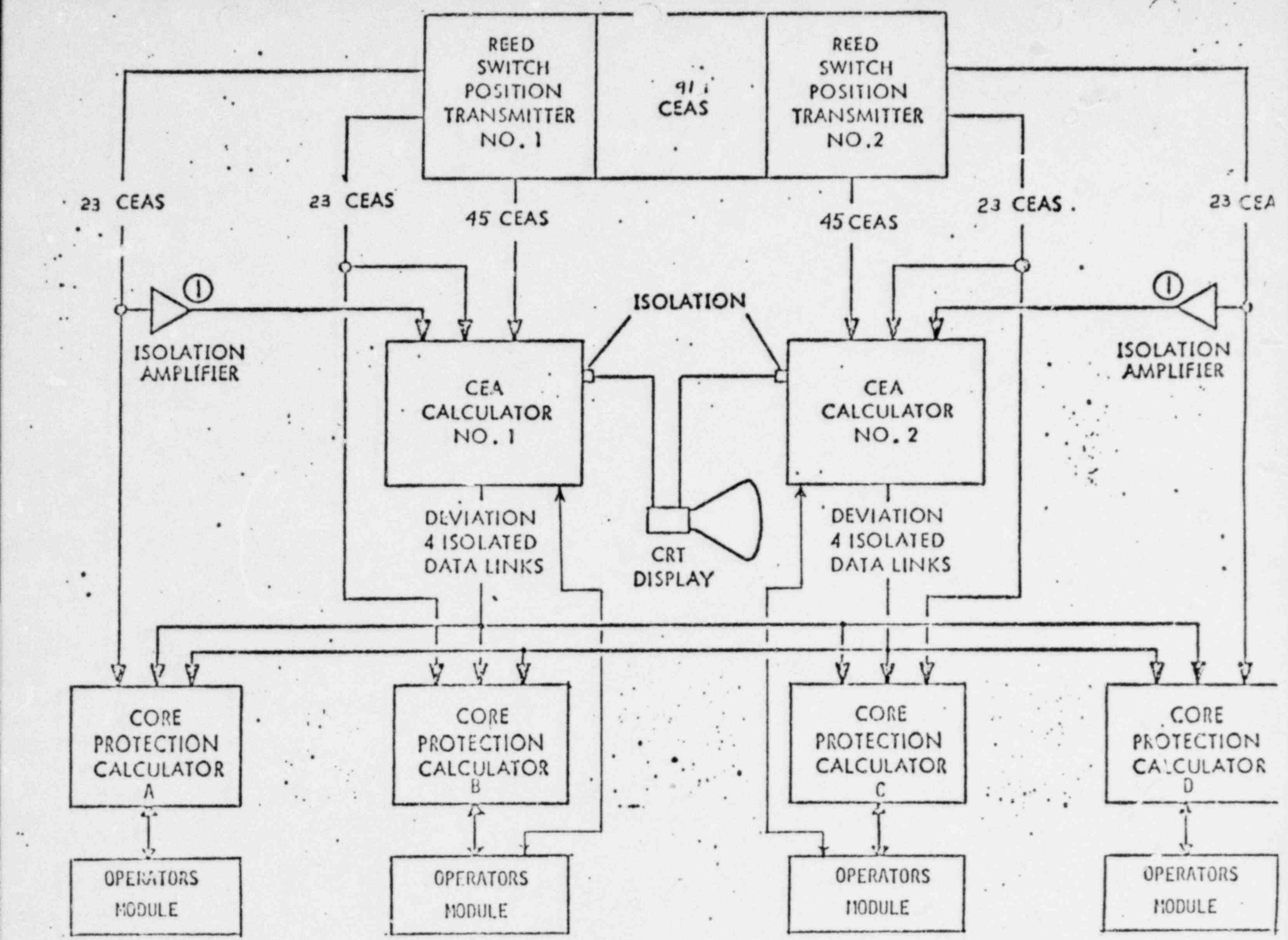
CPC DESIGN BASES EVENTS

MAJOR ANTICIPATED OPERATIONAL OCCURRENCES

1. UNCONTROLLED AXIAL XENON OSCILLATIONS
2. CEA RELATED EVENTS INCLUDING SINGLE ROD WITHDRAWAL, SINGLE DROPPED ROD, SUB-GROUP DEVIATION AND OUT-OF-SEQUENCE WITHDRAWAL AND INSERTION
3. EXCESS LOAD
4. LOSS OF LOAD
5. LOSS OF FORCED REACTOR COOLANT FLOW
6. UNCONTROLLED BORON DILUTION
7. ASYMMETRIC STEAM GENERATOR TRANSIENT DUE TO AN INSTANTANEOUS CLOSURE OF AN MSIV

POSTULATED ACCIDENTS

1. STEAM GENERATOR TUBE RUPTURE
2. REACTOR COOLANT PUMP SHAFT SEIZURE


REED SWITCH POSITION TRANSMITTER NO. 1
91 CEAS
REED SWITCH POSITION TRANSMITTER NO. 2
23 CEAS
23 CEAS
45 CEAS
45 CEAS
23 CEAS
23 CEA
ISOLATION
ISOLATION AMPLIFIER
ISOLATION AMPLIFIER
CEA CALCULATOR NO. 1
CEA CALCULATOR NO. 2
DEVIATION 4 ISOLATED DATA LINKS
DEVIATION 4 ISOLATED DATA LINKS
CRT DISPLAY
CORE PROTECTION CALCULATOR A
CORE PROTECTION CALCULATOR B
CORE PROTECTION CALCULATOR C
CORE PROTECTION CALCULATOR D
OPERATORS MODULE
OPERATORS MODULE
OPERATORS MODULE
OPERATORS MODULE

CPC PROCESS INPUT SIGNALS

SIGNAL	NUMBER PER CHANNEL	RANGE	SIGNAL TYPE
REACTOR COOLANT PUMP SPEED	4	10%-100% RATED SPEED	DIGITAL
COLD LEG TEMPERATURE	2	465-615°F	ANALOG
HOT LEG TEMPERATURE	2	525-675°F	ANALOG
PRESSURIZER PRESSURE	1	1500-2500 PSIA	ANALOG
EX-CORE NEUTRON FLUX	3	0-200 %	ANALOG
CEAC DEVIATION PENALTY FACTOR	2	0-4.0	DIGITAL
TARGET CEA POSITION	23	0-100% WITHDRAWAL	ANALOG

CPC PROTECTION ALGORITHM STRUCTURE

THE CORE PROTECTION SOFTWARE CONSISTS OF FOUR INTERDEPENDENT PROGRAMS AND A TRIP PROGRAM MODULE THAT IS ACCESSIBLE TO ALL FOUR PROGRAMS:

1. COOLANT MASS FLOW PROGRAM (FLOW)
2. DNBR AND POWER DENSITY UPDATE PROGRAM (UPDATE)
3. POWER DISTRIBUTION PROGRAM (POWER)
4. STATIC DNBR AND POWER DENSITY PROGRAM (STATIC)
5. TRIP SEQUENCE PROGRAM (TRIPSEQ)

SAMPLING OF THE INPUT SIGNALS IS INITIATED WITHIN THE PROTECTION PROGRAMS AND IS CONSISTENT WITH THE FREQUENCY OF EXECUTION OF THE CALLING PROGRAM.

MAJOR CALCULATIONS

A. CPC "FLOW" PROGRAM

1. PRIMARY CORE COOLANT MASS FLOW RATE
2. PROJECTED DNBR BASED ON RATE OF DECREASE OF CORE COOLANT MASS FLOW RATE

B. CPC "UPDATE" PROGRAM

1. CORE AVERAGE POWER BASED ON NEUTRON FLUX
2. CORE AVERAGE POWER BASED ON CORE ENTHALPY RISE
3. CORE AVERAGE HEAT FLUX
4. HOT PIN HEAT FLUX DISTRIBUTION
5. DNBR UPDATED FOR CHANGES IN CPC INPUT PARAMETERS
6. PEAK LOCAL POWER DENSITY

MAJOR CALCULATIONS (CONTINUED)

C. CPC "POWER" PROGRAM

1. CORE AVERAGE AXIAL POWER DISTRIBUTION
2. HOT PIN AXIAL POWER DISTRIBUTION

D. CPC "STATIC" PROGRAM

1. STATIC DNBR
2. STATIC HOT CHANNEL QUALITY
3. CORE INLET AND EXIT ENTHALPY

CPC OUTPUT SIGNALS

SIGNAL	TYPE	SETPOINT	RANGE
LOW DNBR TRIP	CONTACT	1.19	——
LOW DNBR PRE-TRIP	CONTACT	1.30	——
HIGH LPD TRIP	CONTACT	393.2*	——
HIGH LPD PRE-TRIP	CONTACT	374.5*	——
SENSOR FAILURE	CONTACT	——	——
DNBR MARGIN TO TRIP	ANALOG	——	0 - 10
LPD MARGIN TO TRIP	ANALOG	——	0 - 25 KW/FT
CALIBRATED NEUTRON FLUX POWER	ANALOG	——	0 - 200 (% OF RATED P(
CORE COOLANT MASS FLOW RATE	ANALOG	——	0 - 2(FRACTION OF REFERENCE FLOW)

* % OF RATED AVERAGE POWER DENSITY (RATED AVERAGE POWER DENSITY IS 5.34 KW/FT)

CPC PROGRAM EXECUTION INTERALS
AND
INPUT SAMPLING RATES

PROGRAM	INPUTS SAMPLED	EXECUTION/SAMPLING INTERVAL
FLOW	1. RC PUMP SHAFT SPEED	50 MILLISECONDS (MS)
UPDATE	1. COLD LEG TEMPERATURES 2. HOT LEG TEMPERATURES 3. PRESSURE 4. CEAC DEVIATION PENALTY FACTORS 5. EXCORE SIGNALS	100 MILLISECONDS (MS)
POWER	CEA POSITIONS	1 SECOND
STATIC	NONE	2 SECONDS

NOTE THAT OPERATORS MODULE DIGITAL DISPLAY IS UPDATED EVERY 0.5 SECOND, SO DISPLAYED VARIABLES FROM "FLOW" WILL BE THOSE FROM EVERY TENTH CALCULATION OF "FLOW"; DISPLAYED VARIABLES FROM "UPDATE" WILL BE THOSE OCCURRING DURING EVERY FIFTH CALCULATION OF "UPDATE".

CORE PROTECTION CALCULATOR SYSTEM

DISPLAY AND INDICATION

OPERATORS MODULE

SYSTEM STATUS INDICATION

OPERATOR DISPLAY OF SETPOINT AND CALCULATED VARIABLES

OPERATING BYPASS CONTROL AND INDICATION

KEYLOCK ADMINSTRATIVE CONTROL FOR CALCULATOR SECURITY

ADDRESSABLE CONSTANT ENTRY FOR CALIBRATION

CPC ANALOG INDICATORS

DEDICATED ANALOG METERS FOR

- DNBR MARGIN TO TRIP SETPOINT
- LPD MARGIN TO TRIP SETPOINT
- CALIBRATED NEUTRON FLUX POWER

ALARM ANNUNCIATORS

STATION ANNUNCIATORS ARE PROVIDED TO INDICATE TRIP STATUS AND OPERABILITY OF THE CPC SYSTEM

ANALOG PROCESS INDICATION

DEDICATED ANALOG METERS DISPLAY EACH CPC SENSOR INPUT VALUES EXCEPT CEA POSITION AND REACTOR COOLANT PUMP SPEED

CEA POSITION DISPLAY

A CRT DISPLAYS THE POSITION OF ALL 81 CONTROL ELEMENT ASSEMBLIES

THE DISPLAY IS SWITCH SELECTABLE TO EITHER OF TWO REDUNDANT SIGNAL CHANNELS.

CPCS

2. COMPARISON OF SAN ONOFRE 2 AND 3 AND ANO-2 DESIGNS

   A. HARDWARE

   B. EXECUTIVE SYSTEM SOFTWARE

   C. APPLICATION PROGRAMS SOFTWARE

CPC HARDWARE COMPARISON

ANO-2 / SONGS

THERE ARE NO DIFFERENCES IN FUNCTIONAL DESIGN OR CRITERIA BETWEEN THE SAN ONOFRE CORE PROTECTION CALCULATOR SYSTEM (CPCS) HARDWARE AND THE ANO-2 CPCS HARDWARE.

THE SAN ONOFRE CPCS HARDWARE IS IDENTICAL TO THE ANO-2 CPCS HARDWARE WITH THE EXCEPTION OF CABLE LENGTHS TO THE OPERATOR'S MODULES AND DISPLAY GENERATOR.

THE TWO PLANTS HAVE DIFFERENT QUANTITIES OF CONTROL ELEMENT ASSEMBLIES (CEAs). THE TWO CPC SYSTEMS, HOWEVER, HAVE THE SAME NUMBER OF ANALOG INPUT MULTIPLEXER CARDS FOR THESE CEAs. THE ANO-2 CPCS JUST HAS MORE SPARE CAPACITY.

CPC/CEAC EXECUTIVE SYSTEM SOFTWARE

COMPARISON ANO-2 / SONGS

THERE ARE NO DIFFERENCES IN THE SOFTWARE DESIGN BETWEEN THE SAN ONOFRE CORE PROTECTION CALCULATOR SYSTEM (CPCS) AND THE ANO-2 CPCS FOR THE FOLLOWING EXECUTIVE SYSTEM FUNCTIONS:

- TASK SCHEDULING
- PRIORITY
- SOFTWARE STRUCTURE

SINCE THE TWO PLANTS HAVE DIFFERENT QUANTITIES OF CONTROL ELEMENT ASSEMBLIES (CEA), DIFFERENCES EXIST IN THE FOLLOWING INPUT/OUTPUT SERVICE ROUTINES:

- READ ALL CEA POSITIONS FROM ANALOG INPUTS
- READ TARGET CEA POSITIONS FROM ANALOG INPUTS
- OUTPUT CEAC BUFFER TO PLANT COMPUTER
- OUTPUT CPC BUFFER TO PLANT COMPUTER

CPC APPLICATION SOFTWARE COMPARISON
ANO-2 / SONGS

DIFFERENCES IN APPLICATION PROGRAMS BETWEEN THE SAN ONOFRE CORE PROTECTION CALCULATOR SYSTEM (CPCS) AND THE ANO-2 CPCS ARE IN THE FOLLOWING MAJOR CATAGORIES:

- DNBR ALGORITHM CHANGES
- DATA BASE CHANGES
- CEA RELATED CHANGES

3. DESIGN, QUALIFICATION AND FIELD STATUS

ITEM	STATUS
1. HARDWARE DESIGN	COMPLETE - 8/76
2. INSTALLED AT SITE	COMPLETE - 6/78
3. FIELD HARDWARE ACCEPTANCE TEST	COMPLETE - 10/80
4. FIELD PREOPERATIONAL TEST	IN PROGRESS, EST. COMPLETION - 4/81
5. CPC/CEAC FUNCTIONAL DESIGN	COMPLETE - 2/81
6. CPC/CEAC DATA BASE	90% COMPLETE: EST. COMPLETION - 3/81
7. SOFTWARE DESIGN	50% COMPLETE, EST. COMPLETION - 3/81
8. SOFTWARE TESTING	5% COMPLETE, EST. COMPLETION 4/81

4. LICENSING STATUS

A. EXTENT OF COMPLIANCE WITH 27 NRC STAFF POSITIONS

B. SER OPEN ITEM

C. OTHER RELEVANT ISSUES

27 NRC STAFF POSITIONS

San Onofre Units ~~1~~ 2 and ~~2~~ 3 design is in full compliance with exception of Position 20 clarification requiring removal of data links between the CPCS/CEAC to Plant Monitoring System (PMS).

SCE Position:

The use of data links outweighs any concerns regarding hypothetical electrical or functional interactions between the CPCS and PMS.

CPCS - SER OPEN ITEM

ITEM	
CPC/CEAC CHANGES ASSOCIATED WITH ADDITIONAL CEAs.	SOFTWARE CHANGES INCLUDED IN CPC/CEAC FUNCTIONAL DESCRIPTIONS CEN- 35, CEN-147, AND CEN-148.
DATA BASE CONSTANTS-UPDATE TO INCLUDE SPECIFIC CORE AND COOLANT SYSTEM DATA.	MAJORITY (60%) INCLUDED IN CEN-149 WORK (90%) COMPLETE NOW.
CHANGES RELATED IMPROVEMENTS IN THERMAL-HYDRAULIC METHODS	SOFTWARE CHANGES INCLUDED IN CPC/CEAC FUNCTIONAL DESCRIPTIONS CEN-135, CEN-147, AND CEN-148.

(MX) Bill Gill - Pink SHIRT

PROPOSED AGENDA

24-25 Feb 1981

ELECTRICAL SYSTEMS SUBCOMMITTEE

STARTED 9 AM. PROMPT.

FEBRUARY 24, 1981

1.	EXECUTIVE SESSION	9:00 - 9:15
2.	Description of the CE Core Protection Calculator and Comparison of the ANO-2 and San Onofre 2&3 Designs (2 hrs) - CE	9:15 -11:15
3.	Discussion of ANO-2 Experience (2 hrs) - Arkansas Power & Light	11:15 - 1:15
	LUNCH	1:15 - 2:15
4.	San Onofre 2&3 Core Protection Calculator (1 hr) - SCE and CE	2:15 - 3:15
	a) Summary of San Onofre Design and Test and Verification Program	
	b) System modifications Use of ANO-2 Experience, and Bases	
5.	NRC Review of the San Onofre Core Protection Calculator (1 hr) - NRC	3:15 - 4:15
6.	Comment by Southern California Edison Company, Arkansas Power and Light Company, and Combustion Engineering	4:15 - 4:45
7.	GENERAL DISCUSSION	4:45 - 5:15

FEBRUARY 25, 1981

DISCUSSIONS RELATING TO THE USE OF COMPUTER PROTECTION SYSTEMS AND CANADIAN REGULATORY REQUIREMENTS FOR REACTOR CONTROL SYSTEMS . . . . 9:00 - COB

Specific questions to be addressed by the NRC Staff as per Dr. Kerr's 12 Feb 81 request:

1) What has been the experience with the use of the data link between the CPC and the plant computer and how would the NRC relate this experience to the NRC's current position on the use of this device?

2) What is ths status of the NRC actions on Arkansas Power and Light request for the continued use of the data link between the CPC and the plant computer?

3) How did the review procedures used for the ANO-2 review differ from the San Onofre 2&3 review? Were features of the San Onofre 2&3 design addressed which were not addressed in the ANO-2 review?

4) Will a FMEA be performed for the San ONofre 2&3 Core Protection Calculator? If not, what is the basis for the decision?

OTHER RELEVANT LICENSING ITEMS

1. SOFTWARE CHANGE PROCEDURE - METHODOLOGY

   A. CEN-39(A)-P, REVISION 2 AND SUPPLEMENT

   B. APPROVED BY NRC

   C. SCE COMMITTED TO USE APPROVED METHOD VIA RESPONSE NRC Q 221.18.

   D. FRAME WORK FOR EXISTING FUNCTIONAL DESCRIPTION AND TEST PROGRAM DOCUMENTATION

2. SOFTWARE TESTING PROGRAM

   A. BEING PERFORMED IN ACCORDANCE WITH CEN-39

   B. RESULTS TO BE PROVIDED TO NRC BY 4/81

Fuzek

CPC SOFTWARE MODIFICATIONS

1. MODIFICATIONS DURING ANO-2 CYCLE 1

2. MODIFICATIONS FOR SONGS

ACRONYMS

ASGT - ASYMMETRIC STEAM GENERATOR TRANSIENT

CEA - CONTROL ELEMENT ASSEMBLY

CEAC - CONTROL ELEMENT ASSEMBLY CALCULATOR

CPC - CORE PROTECTION CALCULATOR

CRT - CATHODE RAY TUBE

ID - IDENTIFICATION

LPD - LOCAL POWER DENSITY

PF - PENALTY FACTOR

RSPT - REED SWITCH POSITION TRANSMITTER

ANO-2 CYCLE 1 CPC SOFTWARE CHANGES

1. ANO-2 FIRST PLANT WITH CPC SYSTEM

   A. ORIGINAL SOFTWARE CONSERVATIVE
   B. CONSERVATISM IMPACTED PLANT PERFORMANCE

2. TWO SETS OF SOFTWARE MODIFICATIONS IMPLEMENTED

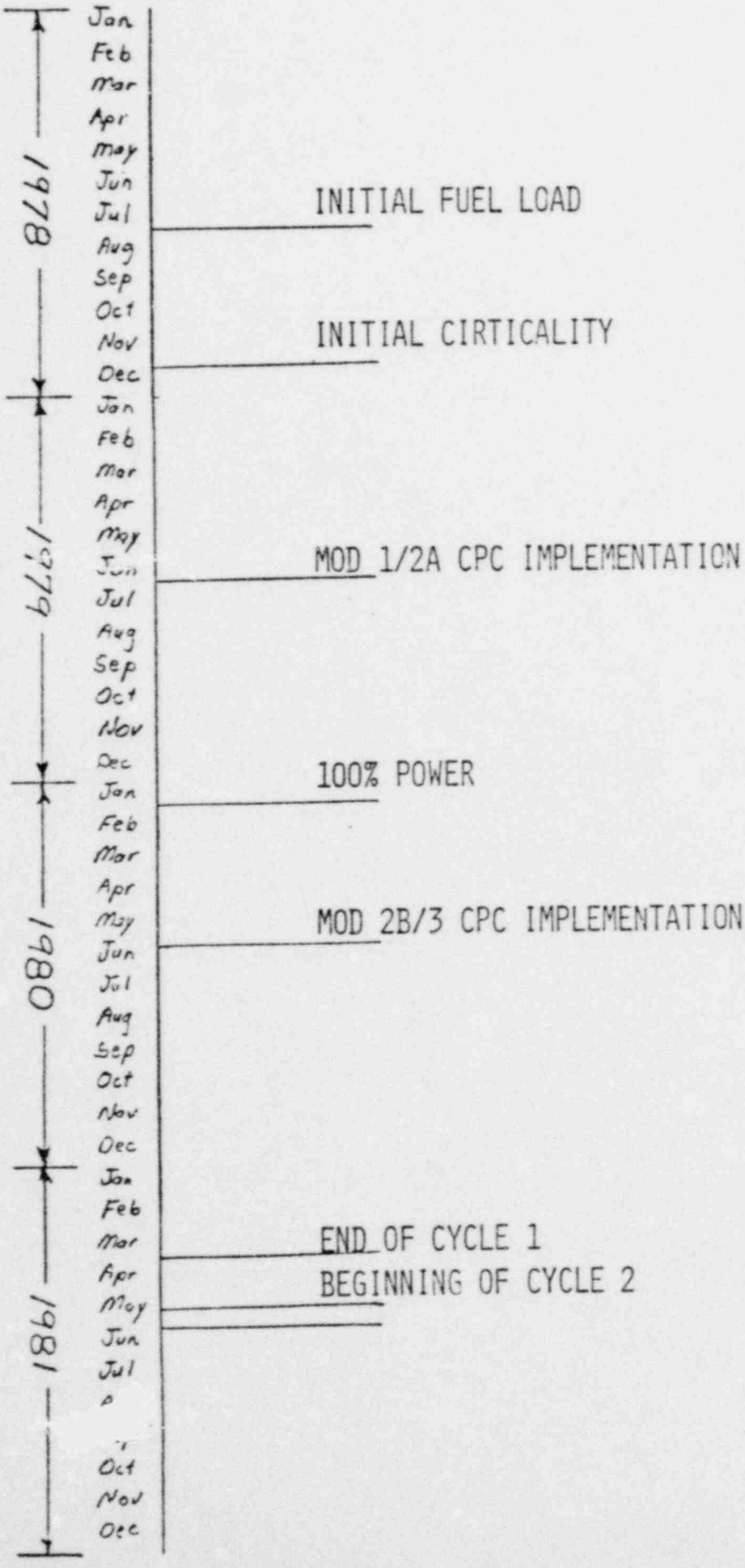
   A. MOD 1/2A

      I. IMPLEMENTED JUNE 24, 1979
      II. CHANGES BASED ON SOFTWARE QUALIFICATION TESTING AND EARLY ANO-2 OPERATION.

   B. MOD 2B/3

      I. IMPLEMENTED MAY 24, 1980
      II. CHANGES BASED ON LATER ANO-2 OPERATION.

3. BOTH SETS OF MODIFICATIONS MADE IN ACCORDANCE WITH THE NRC-APPROVED SOFTWARE CHANGE PROCEDURE, CEN-39(A).


1978
1979
1980
1981
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
INITIAL FUEL LOAD
INITIAL CIRTICALITY
MOD 1/2A CPC IMPLEMENTATION
100% POWER
MOD 2B/3 CPC IMPLEMENTATION
END OF CYCLE 1
BEGINNING OF CYCLE 2

ANO-2 CYCLE 1 SOFTWARE MODIFICATIONS

- LOW POWER FIXED EXCORE SHAPE
- CPC AND CEAC CEA POSITION DEADBANDS
- DYNAMIC THERMAL POWER
- HEAT FLUX AND LPD FILTERS
- FIXED POINT TO FLOATING POINT ARITHMETIC
- CPC AND CEAC INITIALIZATION
- ASGT MODIFICATION
- HEAT FLUX CALCULATION
- *CEAC PENALTY FACTOR CHANGES
- *CPC/CEAC DIAGNOSTICS

---

*DESCRIBED IN FURTHER DETAIL

CEAC PF CHANGES

OBJECTIVE:

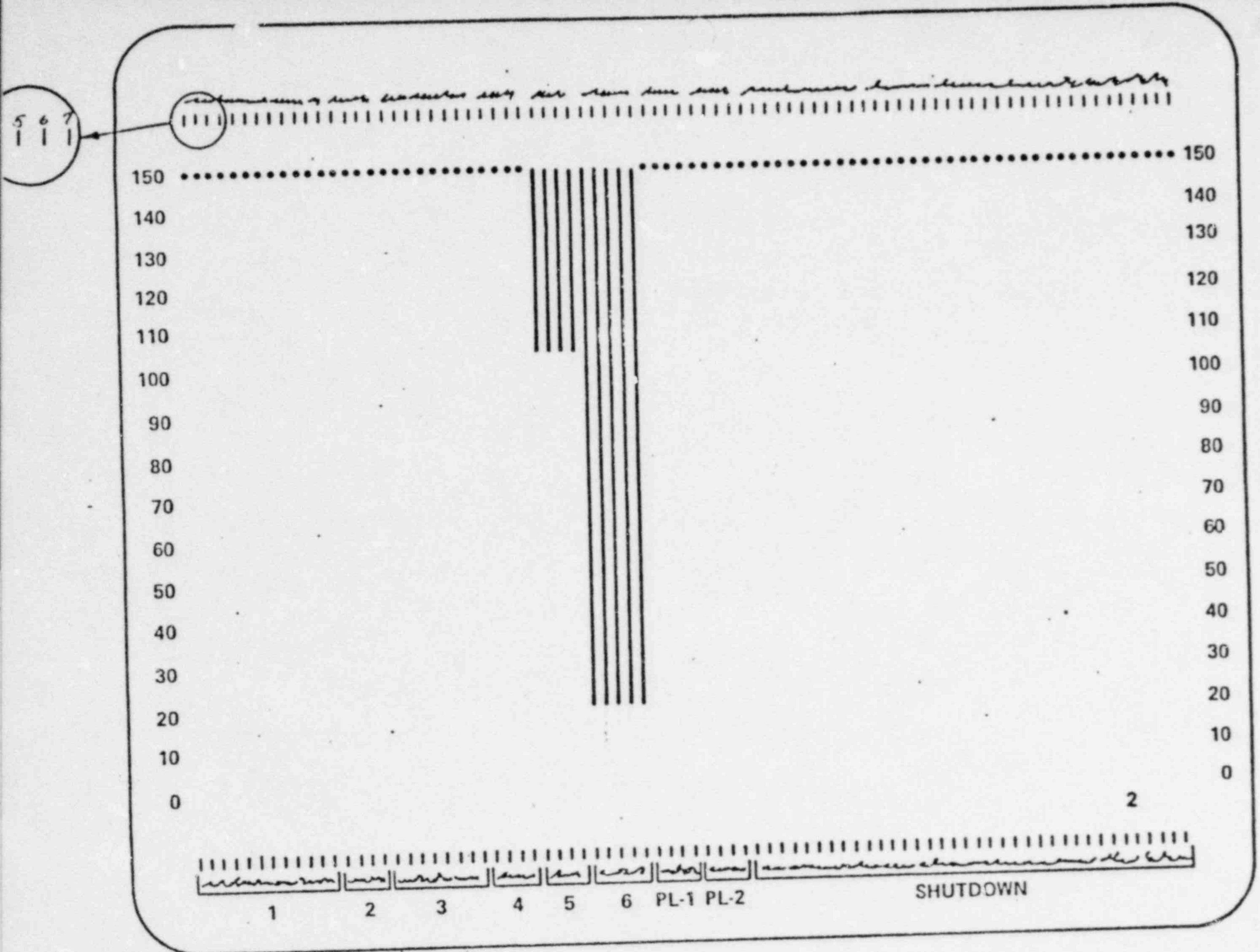
REDUCE THE NUMBER OF UNNECESSARY CPC TRIPS AS A RESULT OF CEA DEVIATION LOGIC.

PREVIOUS DESIGN:

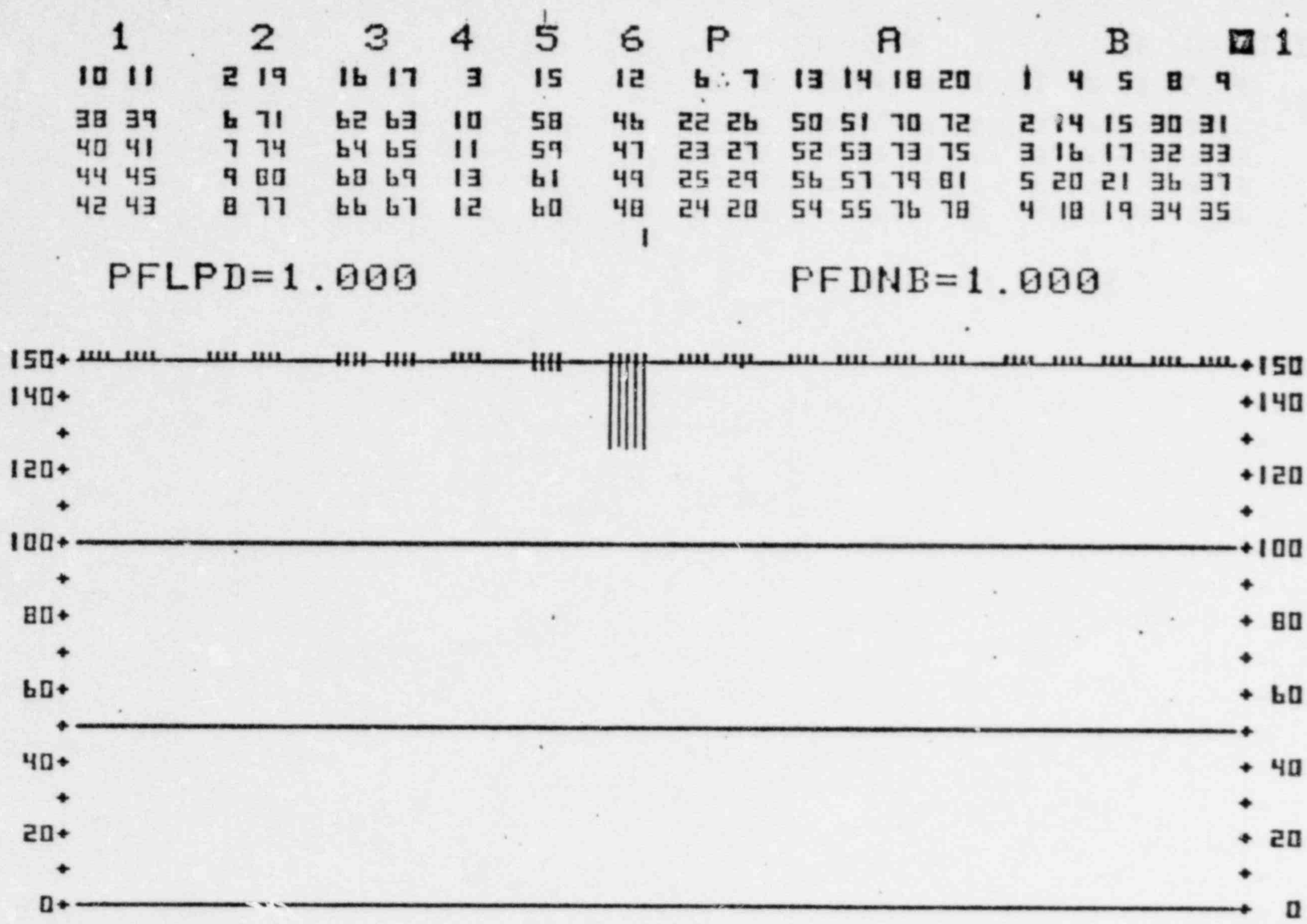
1. THE CEAC CALCULATED ONE "WORST CASE" PENALTY FACTOR WHICH WAS APPLIED TO DNBR AND LPD.
2. THE PF WAS APPLIED TO THE ONE PIN RADIAL PEAK.
3. THE CEAC/RSPT INOPERABLE MODE LOGIC LEAVES BOTH CEACS IN-SERVICE OR TAKES BOTH CEACS OUT-OF-SERVICE.

CHANGES:

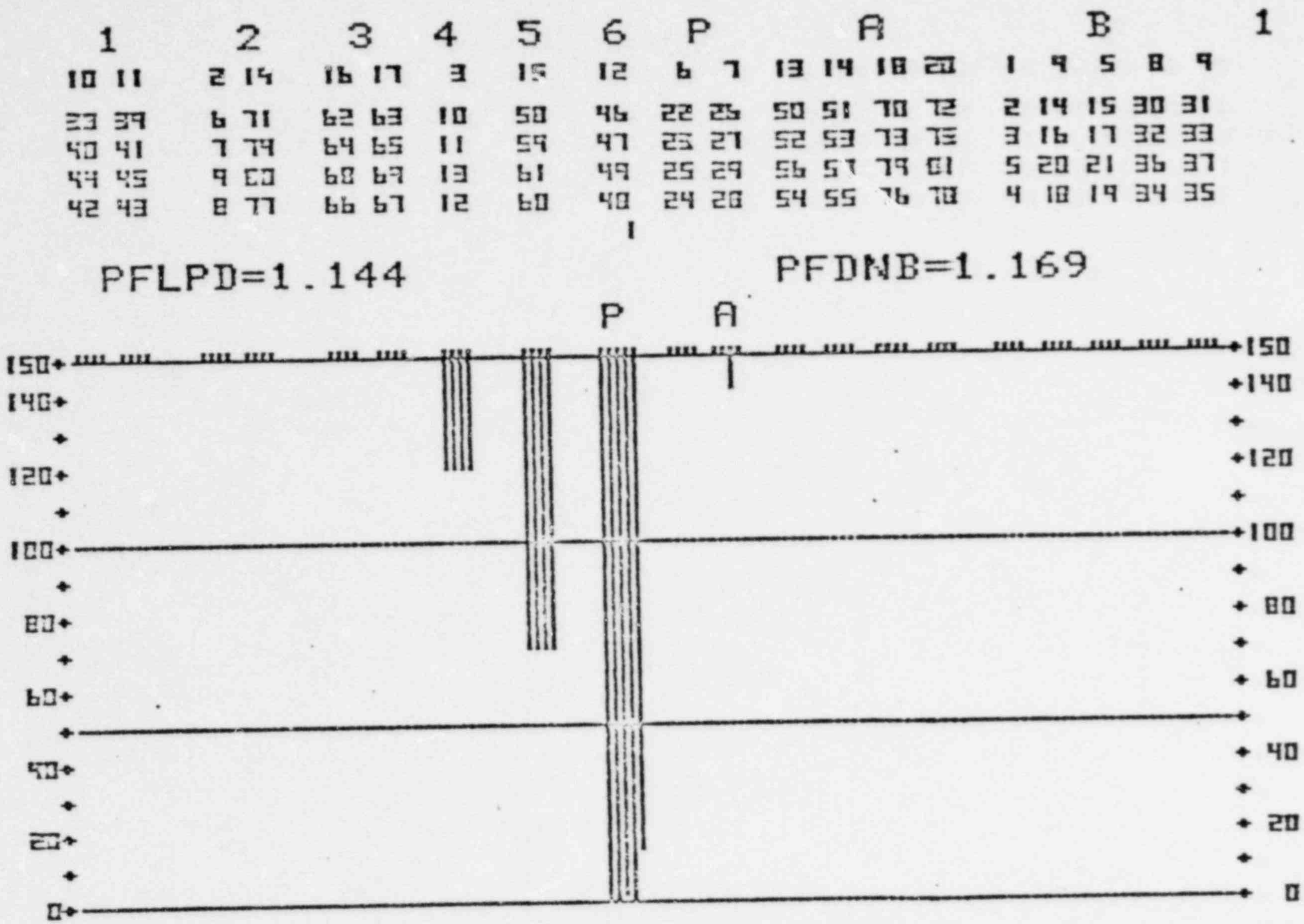
1. SEPARATE DNBR AND LPD PENALTY FACTORS.
2. PENALTY FACTORS DEPENDENT ON:
   - A. MAGNITUDE OF DEVIATION
   - B. DIRECTION OF DEVIATION
   - C. SUBGROUP WITH DEVIATION
   - D. CEA CONFIGURATION
   - E. TIME
3. DATA TRANSMITTED TO CPC FROM CEAC
   - A. FAIL FLAG
   - B. BIG PENALTY FACTOR FLAG
   - C. DNBR AND LPD PENALTY FACTOR
4. APPLY PF TO HEAT FLUX IN STATIC DNBR LOGIC.
5. MODIFY THE CEAC/RSPT INOPERABLE MODE LOGIC SUCH THAT ONE CEAC CAN BE LEFT IN-SERVICE.
6. MODIFY CEAC CRT DISPLAY.



CEA POSITION DISPLAY



CEAC DISPLAY



CEAC DISPLAY

CPC/CEAC DIAGNOSTICS

OBJECTIVE:

PROVIDE ADDITIONAL CPC AND CEAC DIAGNOSTICS TO IDENTIFY THE CAUSE OF SPURIOUS CPC TRIPS.

PREVIOUS DESIGN:

SENSOR STATUS WORDS PROVIDED INFORMATION THAT A CPC SENSOR HAD FAILED.

CHANGES:

1. FAILED SENSOR STACKS IN CPCS AND CEACS

    A. STORES UP TO 6 ENTRIES
    B. CONTAINS SENSOR ID, STATUS, AND TIME OF ENTRY
    C. ACCESSED FROM:

        I. OPERATOR'S MODULE
        II. TELETYPE WHEN CALCULATOR IN-TEST

2. SNAPSHOT OF DATA

    A. CONTAINS INPUTS, ADDRESSABLE CONSTANTS, INTERMEDIATE VARIABLES AND OUTPUTS.
    B. BUFFER FILLED:

        I. IN CEAC, FOR AN OFF-NORMAL PF OUTPUT
        II. IN CPC, FOR A CHANNEL TRIP.

    C. ACCESSED FROM TELETYPE WHEN CALCULATOR IS IN-TEST.

3. LOGIC ADDED TO PREVENT SPURIOUS PENALTIES AS A RESULT OF RSPT ASSOCIATED INSTRUMENTATION ANOMALIES.

SONGS CPC SOFTWARE MODIFICATIONS

- DNBR CALCULATION
- ADDRESSABLE CONSTANTS
- POWER DISTRIBUTION CALCULATION
- DIAGNOSTIC CHANGES
- PLANT SPECIFIC DATA

DNBR CALCULATION

1. STATIC DNBR BASED ON CE-1 CRITICAL HEAT FLUX CORRELATION.

2. UPDATED DNBR BASED ON CE-1 CRITICAL HEAT FLUX CORRELATION.

CPC STATIC DNBR ALGORITHM

OBJECTIVE:

TO INCLUDE A DNBR ALGORITHM WHICH IS CONSISTENT WITH THE DESIGN BASIS THERMAL-HYDRAULIC CODE (TORC).

PREVIOUS DESIGN:

CPC STATIC DNBR BASED ON THE W-3/BULL METHODOLOGY.

CHANGE:

THE STATIC DNBR ALGORITHM BASED ON CE-1/TORC METHODOLOGY.

THE ALGORITHM IS DESCRIBED IN:

CEN-135(S), APPENDIX A, SUBMITTED AUGUST 1980
CEN-147(S), SECTION 4.4, JANUARY 1981

ADDRESSABLE CONSTANTS

1. POWER DISTRIBUTION-RELATED ADDRESSABLE CONSTANTS

    A. CEA SHADOWING FACTOR ADJUSTMENT
    B. PLANAR RADIAL PEAKING FACTOR ADJUSTMENT
    C. BOUNDARY POINT POWER CORRELATION COEFFICIENTS
    D. COOLANT TEMPERATURE SHADOWING FACTOR

2. DNBR AND LPD PRE-TRIP SETPOINTS.

3. AUTOMATED REENTRY OF CERTAIN ADDRESSABLE CONSTANTS.

POWER DISTRIBUTION CALCULATION

1. CHANGE FIXED NUMBERS IN CALCULATION TO DATA BASE CONSTANTS.

2. DENSITY-DEPENDENT RADIAL CORRECTION FACTOR.

DIAGNOSTIC CHANGES

OBJECTIVE:

TO IMPROVE CPC DIAGNOSTICS BASED ON ANO-2 OPERATING EXPERIENCE.

CHANGES:

1. CEAC SNAPSHOT BUFFER
2. FAILED SENSOR STACK ID NUMBERS
3. CEAC CRT REWRITE

Starr

CPC/CEAC
SOFTWARE CHANGE PROCESS

PURPOSE OF PRESENTATION

PRIOR TO THE PRESENTATION ON SOFTWARE MODIFICATIONS TO THE ANO-2 AND SONGS CPC/CEAC SYSTEMS, WE WILL PRESENT THE SOFTWARE CHANGE PROCESS THAT OCCURS WHEN SUCH MODIFICATIONS ARE PERFORMED.

CPC/CEAC
SOFTWARE CHANGE PROCESS

- C-E HAS DEVELOPED A HIGHLY STRUCTURED AND DETAILED CPC/CEAC SOFTWARE CHANGE PROCESS.
- THIS PROCESS IS DOCUMENTED IN THE SOFTWARE CHANGE PROCEDURE CEN-39.
- CEN-39 HAS BEEN APPROVED BY THE NRC STAFF DURING THE RESOLUTION OF STAFF POSITION NO. 19 ON ANO-2.
- CEN-39 HAS BEEN FOLLOWED FOR ALL ANO-2 AND SONGS SOFTWARE CHANGES.
- THE FOLLOWING DISCUSSION COVERS SEVERAL IMPORTANT FEATURES OF THE SOFTWARE DESIGN PROCESS.

CEN-39

SOFTWARE CHANGE PROCEDURE

PURPOSE

TO ENSURE THAT THE PROCESS OF SPECIFYING AND IMPLEMENTING SOFTWARE MODIFICATIONS IS DONE IN A MANNER THAT MAINTAINS THE INTEGRITY AND RELIABILITY OF THE SOFTWARE.

SCOPE

- o FUNCTIONAL DESIGN, SOFTWARE CODING AND IMPLEMENTATION, AND SOFTWARE TESTING ARE COVERED.
- o ALL DOCUMENTS ARE ADDRESSED.
- o WIDE SPECTRUM OF DETAIL IS INCLUDED, FROM RELATIVELY HIGH LEVEL REQUIREMENTS DOWN TO PRECISE, SPECIFIC INSTRUCTIONS FOR DISC GENERATION.

APPLICABILITY

CEN-39 IS APPLICABLE TO ALL SOFTWARE CHANGES.

SOFTWARE DESIGN DOCUMENTATION

DESIGN SPECIFICATION

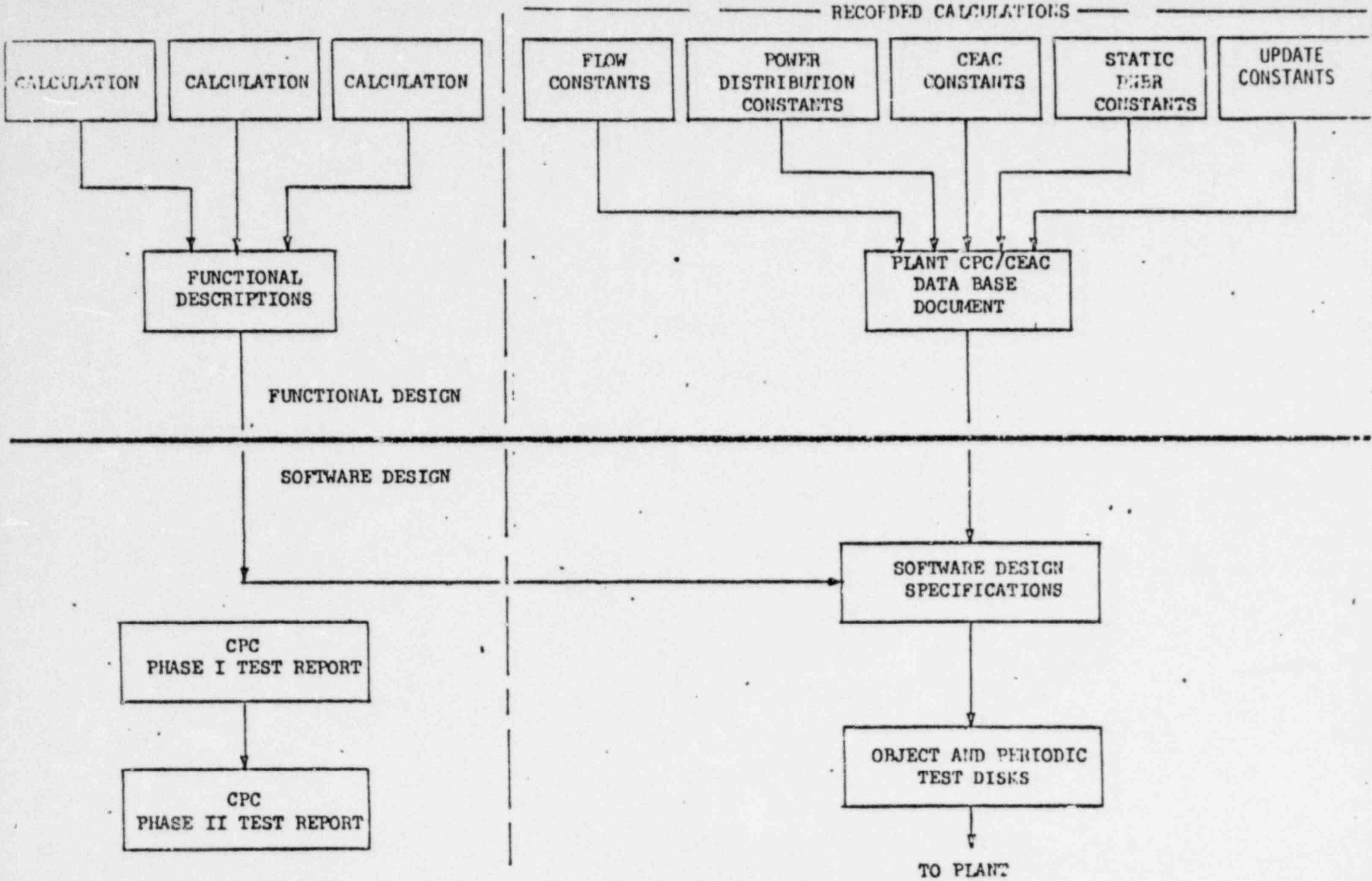
RECORDED CALCULATIONS
CPC FUNCTIONAL DESIGN SPECIFICATION
CEAC FUNCTIONAL DESIGN SPECIFICATION
CPC/CEAC FORTRAN CERTIFICATION
DATA BASE DOCUMENT

DESIGN IMPLEMENTATION

CPC SOFTWARE SPECIFICATION
CEAC SOFTWARE SPECIFICATION
EXECUTIVE SOFTWARE SPECIFICATION

TESTING

PHASE I TEST PROCEDURE
PHASE II TEST PROCEDURE
FLOW TEST CASES
UPDATE TEST CASES
POWER TEST CASES
STATIC TEST CASES
TRIP SEQUENCE TEST CASES
COMMON SUBROUTINE TEST CASES
PENALTY FACTOR TEST CASES
POSITION DISPLAY TEST CASES
PHASE I TEST REPORT
PHASE II TEST REPORT
TEST AND CERTIFICATION ANALYSIS



CPC/CEAC SOFTWARE DESIGN
MODIFICATION BLOCK DIAGRAM

PHASE I TESTING

- VERIFIES THE IMPLEMENTATION OF MODIFICATIONS TO THE CPC/CEAC SOFTWARE.

- IMPLEMENTATION IS THE TRANSLATION OF SYSTEM FUNCTIONAL REQUIREMENTS INTO MODULES OF MACHINE EXECUTABLE CODE, AND THE INTEGRATION OF THESE MODULES INTO A REAL-TIME SOFTWARE SYSTEM.

- ALL MODIFIED MODULES ARE TESTED.

- ALL MODULES THAT ACCESS UPDATED CONSTANTS ARE TESTED.

- TEST CASES ARE SELECTED TO EXCERCISE ALL BRANCHES OF ANY MODULE THAT WAS MODIFIED.

PHASE II TESTING

1. PERFORMED ON A SINGLE CHANNEL CPC/CEAC SYSTEM

2. OBJECTIVES:

   A. VERIFY SOFTWARE MODIFICATIONS HAVE BEEN PROPERLY INTEGRATED WITH CPC AND CEAC SOFTWARE AND SYSTEM HARDWARE.

   B. CONFIRM THAT STATIC AND DYNAMIC OPERATION OF THE INTEGRATED SYSTEM IS AS PREDICTED.

3. BASIS FOR COMPARISON IS THE CERTIFIED CPC/CEAC SIMULATION CODE.

4. TESTS PERFORMED

   A. INPUT SWEEP TEST

   B. DYNAMIC SOFTWARE VERIFICATION TEST (DSVT)

   C. LIVE INPUT SINGLE PARAMETER (LISP) TEST

INPUT SWEEP TEST

1. OBJECTIVES:

   A. DETERMINE PROCESSING UNCERTAINTIES

   B. VERIFY INITIALIZATION OVER OPERATING SPACE

2. MINIMUM OF 500 TEST CASES REQUIRED

3. TEST CASES EXECUTED FOR ANO-2 CYCLE 1

   A. CPC - 2000 CASES

   B. CEAC - 1200 CASES

DYNAMIC SOFTWARE VERIFICATION TEST (DSVT)

1. OBJECTIVES

   A. VERIFY DYNAMIC RESPONSE

   B. FURTHER ASSURE CORRECT SOFTWARE IMPLEMENTATION

2. MINIMUM OF FIVE TEST CASES REQUIRED.

3. EXAMPLE CASES

   - 4 PUMP LOSS OF FLOW
   - SINGLE CEA DROP
   - UNCONTROLLED BANK WITHDRAWAL
   - RAPID DEPRESSURIZATION
   - INCREASING POWER RAMP

LIVE INPUT SINGLE PARAMETER (LISP) TEST

1. OBJECTIVES:

   A. VERIFY DYNAMIC RESPONSE

   B. FURTHER ASSURE CORRECT IMPLEMENTATION OF SOFTWARE

   C. EVALUATE HARDWARE/SOFTWARE SYSTEM

2. MINIMUM OF FIVE TEST CASES REQUIRED

3. EXAMPLE CASES

   - PUMP SPEED SIGNAL RAMP
   - EXCORE DETECTOR SIGNAL RAMP
   - TEMPERATURE SIGNAL RAMP
   - PRESSURE SIGNAL RAMP
   - SINGLE CEA SIGNAL RAMP

SUMMARY

- o A HIGHLY DETAILED AND STRUCTURED PROCESS IS USED FOR SOFTWARE CHANGES.
- o THE PROCESS WAS REVIEWED AND APPROVED BY THE NRC STAFF (CEN-39).
- o CEN-39 WAS APPLIED TO ANO-2 AND SONGS SOFTWARE CHANGES.