OK
SDT

NUCLEAR REGULATORY COMMISSION

IN THE MATTER OF:

THREE MILE ISLAND SPECIAL
INQUIRY DEPOSITION

DEPOSITION OF: STEPHEN H. HANAUER

Place - BETHESDA, MD.

Date - TUESDAY, 25 SEPTEMBER 1979 Pages 1 - 184

Telephone:
(202) 347-3700

ACE - FEDERAL REPORTERS, INC.
Official Reporters 8001240 609

444 North Capitol Street
Washington, D.C. 20001

NATIONWIDE COVERAGE - DAILY

T

CR7093
7247

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

- - - - - - - - - - - - - - - - - - -x
:
In the Matter of: :
:
THREE MILE ISLAND :
SPECIAL INQUIRY DEPOSITION :
:
- - - - - - - - - - - - - - - - - - -x

DEPOSITION OF STEPHEN H. HANAUER

Room P822A
Phillips Building
7920 Norfolk Avenue
Bethesda, Maryland

Tuesday, 25 September 1979
9:00 a.m.

APPEARANCES:

For the NRC:

WILLIAM PARLER
JOSEPH SCINTO
WAYNE LANNING
TOM COX
PETER SICILIA
CHARLES O. MILLER
Members, Special Inquiry Group

For the witness:

PAT DIXON, Office of the General Counsel, NRC.

MADELON
mpb
CR~~70~~93
7247

C O N T E N T S

MPB/ebl

P R O C E E D I N G S

MR. PARLER: Would you please raise your right hand, Dr. Hanauer?

Whereupon,

STEPHEN H. HANAUER

was called as a witness and, having been first duly sworn, was examined and testified as follows:

EXAMINATION

BY MR. PARLER:

Q Please state your name for the record.

A Stephen H. Hanauer, H-a-n-a-u-e-r.

Q Dr. Hanauer, I believe that you have already received a letter from Mr. Rogovin providing you with certain important information regarding your deposition.

MR. PARLER: I would like to mark as an exhibit 1130 a photocopy of a letter which was sent to you.

(Whereupon, the document referred to was marked as Exhibit 1130 for identification.)

BY MR. PARLER:

Q I have given you a copy which I have marked for identification as Exhibit 1130. Is this a photocopy of the letter sent to you by the NRC TMI Special Inquiry Group confirming your deposition here today under oath, Dr. Hanauer?

MPB/eb2

A   Yes, it is.

Q   Have you read the document in full, sir?

A   Yes.

Q   Do you understand the information set forth in this letter, including the general nature of the NRC TMI Special Inquiry, your right to have an attorney present here today as your representative, and the fact that the information you provide here may eventually become public?

A   Yes.

Q   Dr. Hanauer, is counsel representing you personally today?

A   Off the record.

(Discussion off the record.)

Yes, I understand Mr. Dixon with the NRC General Counsel's office represents me personally, as well as the agency.

Q   Dr. Hanauer, you should be aware that the testimony you give has the full force and effect as if you were testifying in a court of law. My questions and your responses are being taken down and will later be transcribed. You will be given the opportunity to look at that transcript and make changes that you deem necessary.

However, to the extent that your subsequent changes are significant, these changes may be viewed as affecting your credibility, so please be as complete and accurate as you can

MPB/eb3

be in responding to my questions.

If you at any point during the deposition don't understand a question, please feel free to stop and indicate that, and we will make the clarification at that time, going off the record as need be for clarifications or for you to locate and refer to documents as necessary.

Okay?

A Yes.

Q I would like to suggest to you two basic groundrules which I'm sure are familiar to you since your deposition has been taken before, as I understand it. One is that you permit me to finish my question before you give your response even if you know what the question is going to be, because the Reporter cannot take down both of us speaking at the same time.

Second, please respond audibly. Motions such as nodding your head cannot be taken down by the Reporter.

Did you bring a copy of your resume with you, Dr. Hanauer?

A Yes.

MR. PARLER: I would like to mark for identification as Exhibit --

THE WITNESS: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

I would like to mark for identification as Exhibit

PB/eb4

1131 a copy of a one-page biographical sketch entitled "Dr. Stephen H. Hanauer, 1979."

(Whereupon, the document referred to was marked as Exhibit 1131 for identification.)

BY MR. PARLER:

Q Dr. Hanauer, does this document which I have marked as Exhibit 1131 for identification, does this accurately summarize your educational and employment background?

A Yes.

Q What is your current position in the Nuclear Regulatory Commission, Dr. Hanauer?

A Director, Unresolved Safety Issues Program, Office of Nuclear Reactor Regulation.

Q What was your position in the Nuclear Regulatory Commission on, say, March 30th, 1979?

A Assistant Director for Plant Systems, Division of System Safety, Office of Nuclear Reactor Regulation.

Q In the position that you occupied on March 30th, 1979, how many people approximately reported to you?

A 45.

Q And what generally were your responsibilities, sir, in that position?

A I supervised three specialized branches: Instrumentation

MPB/eb5

and Control Sys ems, Power Systems, and Auxiliary Systems, and the review of license applications for construction permits and operating licenses.

Q Dr. Hanauer, to whom did you report in that position?

A Dr. Roger Mattson, Director of the Division of System Safety.

Q In your present position, sir, approximately how many people are involved under you?

A This answer has to be more complicated. I have supervision over 20 task groups for the 19 unresolved safety issues, and one other issue considered to be very important. These efforts involve upwards of 50 people who, however, report directly to their line supervision as well as participating in the task groups under my supervision.

Q For the purpose of the record, at this point would you mention the one other thing in addition to the 19 I believe issues that you said you were concerned with?

A Issue B6, load combinations.

Q Which generally, without going into details, is concerned with what?

A It's concerned with the methods of combining structural response to the loads imposed by different events which could occur concurrently such as earthquakes and accidents of other kinds.

Q Dr. Hanauer, in your current position, to whom do you

/eb6

report?

A Mr. Harold Denton, head of the Office of Nuclear Reactor Regulation.

Q Dr. Hanauer, we have your resume but I would like to go over some of the points that are made in that resume for the purpose of the record at this point.

Would you, for the record, state your educational background, please, Dr. Hanauer?

A I have bachelor's and master's degrees in electrical engineering, and a Ph. D. in physics.

Q Now prior to joining the Nuclear Regulatory Commission, what was your employment background? I gather that in the 1950s you were employed at the Oak Ridge National Laboratory. If that is correct, sir, would you so indicate and state for the record generally what that employment history involved?

A Well, as stated in my biographical sketch, I was employed from 1950 to 1965 at the Oak Ridge National Laboratory. During almost all of that time I was involved in reactor instrumentation and control in various capacities: designing systems, developing and testing components, establishing safety and operating requirements.

And during the last five years I supervised the group that was charged with developing reactor instrumentation of different kinds and for new purposes.

Q During that period were you issued any patents,

MPB/eb7

Dr. Hanauer?

A Yes, one.

Q Was that in the area that you just described?

A Yes, it was for a system for automatic reactor start-up.

Q And then after your employment at the Oak Ridge National Laboratory, then you moved into the academic world. Is that true, sir?

A That is correct. I was professor of Nuclear Engineering at the University of Tennessee from 1965 to 1970.

Q During that period of time I gather that you were also a member of the Atomic Energy Commission's Advisory Committee on Reactor Safeguards. Is that correct, sir?

A That is correct.

Q That was for a period of what, about five years?

A About five years.

Q And during that period you served as the Chairman of the Advisory Committee on Reactor Safeguards, and also the Vice Chairman of the Advisory Committee on Reactor Safeguards. Is that correct, sir?

A That's correct. I was Vice Chairman for calendar year 1968, and Chairman for calendar year 1969.

Q You also were employed with the United States Atomic Energy Commission after your tour ended as a member of the Advisory Committee on Reactor Safeguards. Is that correct?

MPB/eb8

A More or less. I accepted full-time employment with the Atomic Energy Commission in June, 1970, and resigned from the Advisory Committee on Reactor Safeguards when I took up full employment. The two activities were not compatible.

Q What was your first position with the Atomic Energy Commission, please, Dr. Hanauer?

A I was technical advisor to the Director of Regulation.

Q And you held that position for how long, sir?

A In substance, for nine years; in name for approximately two years. When Mr. Muntzing because Director of Regulation the title of the position was changed to Director of the Office of Technical Advisor. This name persisted until the termination of the Atomic Energy Commission in January, 1975.

When the Nuclear Regulatory Commission was formed, I was appointed to an essentially identical position as technical advisor to the Executive Director of Operations.

Q What, generally, were your responsibilities as technical advisor to the Director of Regulation of the Atomic Energy Commission?

A I was to provide counsel on technical matters to the Executive Director. This involved a degree of cognizance and surveillance of all the technical activities and, in particular, the technical problems of the then regulatory staff of the Atomic Energy Commission.

I was principally directed and interested toward

MPB/eb9

reactor safety problems, but did get involved in some of the others as appropriate. I performed investigations; I chaired test groups; I participated in various studies and made recommendations to the Director of Regulation and to other management and organization units of the regulatory staff and on occasion, to the Commission.

Q Your responsibilities were essentially the same, or were they changed when you headed the Office of Technical Advisor which was established by Mr. Muntzing?

A They were essentially the same. They were somewhat broadened in that a small technical staff was included and somewhat later, the Applied Statistics Branch was added to my responsibilities. But the over-all duties could be described in pretty much the same terms.

Q Now from January, 1975, when the Nuclear Regulatory Commission was created, until some time in 1978, when you assumed your position as the Assistant Director for Plant Systems in the Division of Systems Safety, Dr. Hanauer, you have said that you were the technical advisor to the Nuclear Regulatory Commission's Executive Director for Operations. Is that correct, sir?

A That is correct.

Q And your duties in that position, were they essentially the same as you have already described?

A That is correct.

MPB/eb10

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. PARLER:

Q With the details that have been given in your resume, Dr. Hanauer, that you have elaborated on in response to my questions, I think it is fair to say that you have had long experience with the -- just about every aspect of the regulatory process of the Nuclear Regulatory Commission and its predecessor. Is that correct, sir?

A That's correct, except that I've not participated in any licensing hearings. I have participated in one rule-making hearing.

Q You have had the opportunity, though, in positions of responsibility to observe the licensing and regulatory process from the perspective of the Advisory Committee on Reactor Safeguards, from the perspective of a senior position, advising the Atomic Energy Commission's Director of Regulation, the Nuclear Regulatory Commission's Executive Director for Operations, and also now in a responsible line position in the Division of System Safety. Is that correct, sir?

A That's correct.

Q So you have been in a position over the years so that you are familiar with and perhaps have been an important part of the development of licensing and regulatory policy. Is

MPB/eb11

that correct, sir?

A Yes.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. PARLER:

Q Dr. Hanauer, during your service on the Advisory Committee on Reactor Safeguards, were you involved in the Advisory Committee on Reactor Safeguards' review of the Three Mile Island Nuclear Station, Unit Number 2?

A Yes.

MR. PARLER: I will mark for identification as Exhibit 1132 a letter dated July 17, 1969, to The Honorable Glen T. Seaborg, U. S. Atomic Energy Commission, Subject: Report on Three Mile Island Nuclear Station, Unit Number 2. This letter was signed by Dr. Stephen H. Hanauer, who was then the Chairman of the Advisory Committee on Reactor Safeguards.

(Whereupon, the document referred to was marked as Exhibit 1132 for identification.)

BY MR. PARLER:

Q I hand you a copy of this letter, Dr. Hanauer.

(Document handed to the witness.)

Have you had the occasion in recent months to re-read

MPB/eb12

this letter to refresh your recollection?

A No.

Q I wonder if you'd mind doing so. What I would like to do is to see now, over a decade ago, at least this part of the process worked to identify things which appeared to be of safety significance about this plant at its construction permit stage.

A Off the record.

(Discussion off the record.)

BY MR. PARLER:

Q What were the concerns, if any, at the construction permit stage of Three Mile Island, and were the concerns expressed in the letter dated July 17, 1969, which has been marked as Exhibit 1132?

A Well, in direct answer I will have to say that I no longer remember in any detail the concerns on this particular plant, but they are embodied in the report of the Committee, Exhibit 1132. In general, the ACRS does not conduct a complete, detailed review of each plant, but identifies two sorts of concerns for each of its reviews.

One is any particular feature of the individual plant which the Committee believes warrants its looking into. And the second is to use the successive plants to make progress and improvements in areas of safety of general concern to the Committee at that particular time.

1.262

MPB/eb13

Viewed in that context one can read the 12 technical paragraphs of this report to -- I'm sorry, correction -- 11 technical paragraphs of this report and recall, based on this letter, the underlying concerns, paragraph by paragraph.

The first technical paragraph which is the second paragraph of the letter relates to the Three Mile Island site which is near an airport, and for which, just as Unit 1 on this site, hardening was required for postulated aircraft crashes.

The second technical paragraph relates Three Mile Island Unit 2 to Three Mile Island Unit 1 in a fairly general way and states the Committee's belief that resolution of generic matters applicable to Unit 2 should be pursued.

Off the record.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

THE WITNESS: The following paragraphs consider a number of technical matters related to this particular plant. I will only enumerate them and we can go on.

The third paragraph discusses the design basis flood.

The fourth paragraph discusses the design of the containment and in particular the grouted tendons in the pre-stressed containment design.

The next paragraph discusses the containment spray

MPB/eb14

chemical additive to improve iodine removal.

The next paragraph discusses the possibility of hydrogen buildup in the containment.

BY MR. PARLER:

Q Dr. Hanauer, at that point, recognizing that this record that we are making here some day may be read by laymen, and also understanding that I am a layman asking you, the expert, the question, in view of the reference in the paragraph that you just alluded to, to hydrogen buildup from various sources in the unlikely event of a loss-of-coolant accident and the fact that that issue was considered over a decade ago, why would it appear that at the Three Mile Island accident that there was the concern about-- The hydrogen issue there was apparently a novel concern and an unexpected concern. In other words, could you try to relate the hydrogen buildup issue here in this letter to the hydrogen issue which presumably was involved in the Three Mile Island 2 accident?

A Yes.

The concern in the ACRS report related to hydrogen buildup -- generation rather than buildup. hydrogen generation from the chemical reaction of the Zircaloy fuel cladding and water or steam in the core in the event that the core would be overheated. This hydrogen generation is a fact of nature. The chemical reaction rate is strongly dependent upon the temperature.

The concern that the ACRS was dealing with in 1969 was the amount of hydrogen that could be built up in the containment and the possibility of the reaction of this hydrogen with the oxygen in the air in the containment atmosphere.

Two concerns related to hydrogen actually occurred in the Three Mile Island accident in 1979. The first one chronologically was almost precisely as predicted in 1969. The core did become overheated. The chemical reaction between the Zircaloy and water did take place. A large amount of hydrogen was generated. This hydrogen did escape to the containment and the pressure spike in the containment is universally believed to be evidence that the hydrogen and the oxygen did combine chemically to release a substantial amount of energy.

2

The second hydrogen concern in the Three Mile Island accident related to the buildup of hydrogen gas inside the primary system and was not foreseen in the ACRS or other reviews ten years ago.

Q Do you have anything else to add about the other technical paragraphs in the letter? In other words, continue as you were before I interrupted you to ask the question about the hydrogen.

A Yes, I'll go through them briefly one by one.

Q Briefly.

A The next paragraph relates to the instrumentation of the reactor for the potential for common failure modes, and the

MPB/eb16

consequences of interconnecting the control and safety instrumentation.

The next paragraph relates to possible failure of the scram system during anticipated transients, the so-called ATWS issue.

The next paragraph relates to vibration or loose parts in the reactor system during operation and means for detecting this anomaly if it should occur.

The next paragraph relates to long-term viability of the emergency core cooling system after the postulated loss-of-coolant accident.

And the final technical paragraph relates to the design, inspection, and integrity of the fly wheels on the main coolant pumps.

Q Good.

Some people are under the impression or may be under the impression that the regulatory process, vendors, the ACRS in past years did not consider, perhaps at all, small break LOCA analysis. Would that be a correct understanding? In other words, was it not considered at all? Or is there something else that is involved about the -- Maybe the small break LOCA analyses were considered but there are questions that later on have come up about the adequacy of the consideration?

A The small break LOCA was included in the consideration of loss-of-coolant accidents and emergency core cooling

MPB/eb17

requirements. It is included in the ECCS rule, 10 CFR 50.46 and 10 CFR 50, Appendix K.

However, the great difficulty in delineating the large loss-of-coolant accident led to an unjustified complacency that the small break was well in hand, that the models used to calculate the course and consequences of small-break accidents did not require anything like the degree of attention that these same matters occupied for large breaks.

I think the consideration of small breaks since the Three Mile Island accident has shown that they received inadequate attention before the accident.

Q Dr. Hanauer, I have a letter dated October 22nd, 1976, from Dade W. Moeller, who was the Chairman of the Advisory Committee on Reactor Safeguards. The letter is to The Honorable Marcus J. Rowden who was then the Chairman of the Nuclear Regulatory Commission, Subject: Report on Three Mile Island Nuclear Station, Unit Number 2.

MR. PARLER: This is a letter which I will mark for identification as Exhibit 1133. It's the ACRS letter on Three Mile Island at the operating license stage.

(Whereupon, the document referred to was marked as Exhibit 1133 for identification.)

BY MR. PARLER:

PB/eb18

Q Dr. Hanauer, I realize of course that in 1976 you were not on the ACRS.

I will show you the letter, however for a different purpose.

(Document handed to the witness.)

Again, looking back to your days and years on the ACRS, could you tell me from your experience how the Committee relates or follows up on what its views are as expressed in its letter at the construction permit stage of a plant, how those things have been treated or are treated at the operating license stage?

A When the Committee reviews an application for an operating license it's a number of years, in this case seven years, after the Committee has reviewed the application for a construction permit. During this time it is reasonable to suppose that the problems in the forefront of the Committee's consideration are quite different from the ones that had occupied it seven years earlier.

The Committee always looks at its construction permit letter when it issues a report on the operating license application. But in general, the problems that appear to the Committee at the operating license stage are rather different. This is not always the case.

For example, the operating license report, Exhibit 1133 contains a paragraph related to anticipated transients

PB/eb19

without scram, an issue that was in the construction permit report.

There's a paragraph about the design basis flood in the operating license letter, although the emphasis is on the plans rather than the definition of the flood itself.

There is a paragraph on post-accident operation with somewhat different emphasis than the paragraph on the same subject in the construction permit review.

There is a paragraph related to the resolution of generic issues which is somewhat different in character than that in the construction permit review, reflecting the passage of seven years.

And the rest of the four-page operating license Committee review relates to problems not included in the construction permit review. Part of this is the change in Committee focus onto current problems and the resolution of the ones that had been current seven years previously.

Part of it is the change in focus from a construction permit perspective to an operating license perspective in which the plant has been designed and constructed and operating procedural and management questions become more immediate concerns than they were seven years previously.

Q Dr. Hanauer, I'd like to ask you a very general question. This question also is asked to you in the ACRS context and that is if you would try to recall a decade or so ago when

MPB/eb20

you were on that Committee.

How did the Committee, the Advisory Committee on Reactor Safeguards during your time on that Committee go about establishing the importance of things which that Committee thought should be emphasized for purposes of protecting the public health and safety?

A This was determined partly by the individual and the collective judgments of the Committee members, tempered by the judgment of the Staff as shown by the issues they would emphasize in their reviews, and the questions and problems they would explicitly refer to the Committee for its advice.

We had at that time no quantitative probabilistic framework to use in establishing the relative importance, priority risk contribution of various technical issues we were dealing with, and so we used our judgment.

Q Incidentally, Dr. Hanauer, can you recall now whether the integrated control system of the B&W plants was looked at, considered by the ACRS during these later years in the 1960s in the review of Three Mile Island and Oconee?

A The integrated control system did not have its present form at that time. An earlier version was available and there were of course control systems on the earlier Babcock and Wilcox plants.

Control and instrumentation systems is an area where I've done a great deal of professional work myself and so I

MPB/eb21

would rather naturally tend to pay attention to them.

At that time, however, and until quite recently it was generally believed, and I believed, that control systems merited a somewhat lesser emphasis in a safety review, that although control systems were very important to the reliable and economical operation of the plant and it was recognized that control system failure could initiate the need for protection system action, it was not believed necessary to study the details of control system design and performance.

I still believe that this is largely true although it is clear from the Three Mile Island accident and many other things that the almost total neglect of control systems in safety review was probably not the right thing to do and that more attention should have been paid to it.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

I have handed to Dr. Hanauer a document which I will mark for identification as Exhibit 1134.

(Whereupon, the document referred to was marked as Exhibit 1134 for identification.)

MR. PARLER: This document is entitled "A Report to the Atomic Energy Commission on the Reactor Licensing Program

MPB/eb22

by the Internal Study Group, June 1969." The words that I have given are on the cover page of this document.

BY MR. PARLER:

Q Dr. Hanauer, it's my understanding that the document that I have given to you is a study under the chairmanship of Harold G. Mangelsdorf who was then a member of the ACRS, and that you as a member of the ACRS, indeed the Chairman of the ACRS, participated in that study. Is that correct, sir?

A That's correct.

Q Could you tell me generally what your recollection is that the purpose of this study was? That is the question, but let me add a couple of thoughts to it that would give the question better perspective.

I think that we are familiar with any number of studies that have been conducted over the years to look at the efficiency of the licensing process, improving the schedules, et cetera. It is my understanding that this study which has come to be referred to I believe as the Mangelsdorf study, that one of his main purposes was to focus on the technical review part of the licensing process, in other words, the quality of the technical review.

I'll ask the question again: Is that the main purpose that you recall of this study, or if not, could you please describe generally the purpose of the study as you recall it?

A That's my understanding, and that was the charter of

PB/eb23

the panel as given by the Commission.

Q Incidentally, Dr. Hanauer, do you recall any similar studies that had, say, been chartered by the NRC ACRS -- similar in-depth studies of the technical review process, or is the Mangelsdorf study one that, to some extent at least, stands alone?

A There have been others. The so-called Denton study included a searching consideration of many aspects of the technical review process and how it could be improved. The recommendations were procedural in form, but the objective was the same, to improve and technical review and also the efficiency of this review.

Q So the Denton report, which I believe was issued in the late spring or early summer of 1977, and the Mangelsdorf report, which was issued to the Atomic Energy Commission in 1969, are the two studies which stand out in your mind as being the more thorough studies dealing with the quality of the technical review. Is that correct, sir?

A That's correct. They had somewhat different emphases but they dealt in this way.

Q Now I have reviewed this document, the Mangelsdorf study, Dr. Hanauer, and it would appear that some of the conclusions and recommendations of that study were not only pertinent then but they remain pertinent today. If you don't mind, I would like to refer you to a number of them and ask for your

MPB/eb24

comments on them in the vein of where things stood, say, at the time these recommendations were made and where things stand now.

I realize it has been a long time since you participated in the study.

Incidentally, have you had occasion to review this report recently?

A No.

Q Well, then the record should reflect that, and also that some of the discussion, your responses, would have to be understandably general, or maybe you wouldn't have any comment to make at all on any of these things.

Could we proceed on that basis?

A Yes.

MR. DIXON: Off the record.

(Discussion off the record.)

MR. DIXON: Back on the record.

BY MR. PARLER:

Q On page 8 of the Mangelsdorf study, one of its first recommendations had to do with the development of regulatory criteria and standards relating to safety and, among other things, the study pointed out that:

"While more technical information is needed before the development of comprehensive regulatory criteria can be completed, the group believes that

MPB/eb25

the basic organizational structure and technical capability for developing the needed industry safety codes and standards already exists."

A Where are you reading from?

Q I'm reading from page 10.

Do you have any general comment on the adequacy of regulatory standards, regulatory criteria and standards relating to safety? Are these things woefully inadequate, adequate, more than adequate? In other words a comment in that context?

A Well, since 1969, we've seen the following series of events:

First we've had the general design criteria, 10 CFR 50, Appendix A.

Then we've had a series of over 150 guides related to reactor safety review, as well as a large number on other subjects.

We've had the development of a large number of consensus standards, incorrectly called here and elsewhere industry standards, promulgated principally by the technical engineering societies and the American National Standards Institute.

We've had the development of the standard formats and contents of Safety Analysis Reports.

We've had the development and implementation of the several-thousand-page Standard Review Plan.

MPB/eb26

So that in fact there has been what I would characterize as an enormous increase compared to 1969 in the amount of regulatory criteria and standards relating to reactor safety.

I think this has been a large step forward in the effectiveness as well as the efficiency of the technical review of reactor safety, and that we were right in 1969 to call for the development of this body of standardization documents.

Q So there has been progress, considerable progress?

A Oh, yes. I wouldn't want to imply that it was perfect or that nothing else is needed, but there has been a revolution in the amount of guidance and standardization available to the designer and the safety reviewer since 1969.

Q Now if you would turn to the second area that is dealt with in the Mangelsdorf report on page 12? The title of that recommendation is "Differing Views on Reactor Safety Requirements." I'm reading from the top of page 12 now, for the record. Of course you're reading it yourself.

> "There are differences of opinion on the degree of reliance that should be placed on the reactor system itself and on engineered safety features, the number of such features required and the kinds of failures to be considered. There are differences of opinion on whether and to what extent trade-offs can be made on the various safety elements."

MPB/eb27

THen on this page the recommendation apparently is that:

"The Commission should adopt a policy that the greatest emphasis and priority be placed on the application of quality assurance to the design, construction and operation of nuclear plants so as to achieve the exacting level of safety required."

Take your time to read the page but after you do so, Dr. Hanauer, I wonder if you would comment on this particular recommendation.

3

A Yes. There are several currents of thought embodied here. There was at that time a strong attack against the principle of defense in depth and the apparently inconsistency and, in many cases actually inconsistency to requirements which resulted. Commissioner Ramey and Mr. Shaw, who was head of the Division of Reactor Development and Technology, both expressed the belief that the entire or nearly the entire reliance on safety should be placed on doing the job right in the first place, and the quality assurance program that goes along with it, and deprecated including improbable accidents as part of the defense in depth.

This section is a response to that. The panel's response was to acknowledge and even emphasize the value and necessity of a quality assurance program which at that time was not well delineated and was not embodied in the Commission's

MPB/eb28

regulations.

But at the same time, the panel did not agree with the point of view that the defense in depth, the redundancy, the hypothesis of severe design basis accidents was unnecessary and overconservative. And this is the reason for the discussion of differing views in this section.

Q All right.

Do you believe that this recommendation that the greatest emphasis and priority be placed on the application of quality assurance, that that policy, that is, emphasizing quality assurance, has been adequately reflected in the regulatory program of the Nuclear Regulatory Commission? Does quality assurance get the priority attention it deserves in the regulatory program?

A Perhaps more than it deserves. I think the pendulum has perhaps swung too far and that a very large mountain of quality assurance documents is taken to be compliance with the spirit of this and other discussions of the overriding necessity for adequate quality assurance.

If one views quality assurance in the broadest sense as we were perhaps doing on the Mangelsdorf panel ten years ago, then my opinion would be unchanged, that quality assurance in design, construction and operation of nuclear power plants is essential, in particular in the owner's program to design, construct and operate the plant in a safe way.

MPB/eb29

Just as the Nuclear Regulatory Commission can't look at everything, the owner can't look at everything either and has to have in place a detailed quality assurance program that does look at everything.

On the other hand, if you will look at the failures and mistakes that add up to the Three Mile Island accident, you have to say that only in the broadest view do they represent quality assurance failures in the sense that a perfect quality assurance program would catch all mistakes and all errors.

The procedures at Three Mile Island, for example, made it easy for the operators to make some of the mistakes which they made, which created and aggravated the accident. The procedure for testing the auxiliary feedwater system made it easy to leave it turned off. And the procedure for manipulating the high pressure injection system made it easy to turn it off when the pressurizer level instruments showed the pressure to be full and implied an inappropriate inference that the reactor was full.

Therefore, I would have to say that one can only could to a certain degree on a quality assurance program and that I don't think I would write the system just the same today, the section the same today, although the opinions in it, taken one by one, I still subscribe to.

Q The next discussion and recommendation in the

MPB/eb30

Mangelsdorf report is on page 16. Safety research is related to the licensing of power reactors. It would appear that at least to some extent the discussion -- the emphasis was on the research that is associated with the construction permit and that needs to be completed prior to the issuance of the operating license.

Beyond that there was perhaps some more general discussion of safety research for power reactors.

Do you want to read this section to refresh your memory about this section, Dr. Hanauer?

A I'm doing it as you go along.

Q Okay. Why don't you just take your time and look at it.

(Witness reviewing document.)

A All right.

Q Well, there has been some concern expressed over the years about the adequacy of the research program for licensed commercial nuclear power reactors, what the government's role should be, what the industry's role should be, et cetera.

Now I gather that sort of thing is also covered in this recommendation. Is that right?

A This recommendation was born out of frustration. The AEC's safety research program was demonstrably inadequate and unresponsive to the needs of the ACRS and the regulatory staff during this period. There's a large number of ACRS reports to

MPB/eb31

the Chairman of the AEC in which a large number of recommendations were made on safety research, a large fraction of which were not implemented by the Atomic Energy Commission.

That situation persisted until the formation of the Reactor Safety Research Division in the AEC under Dr. Ray's chairmanship.

The point of this section in the report is in Item 3 on the top of page 17, which I will read into the record.

"If necessary, research programs are not being conducted or are not sufficiently responsive to the identified needs. Alternative courses of action should be developed and implemented by the AEC and the nuclear industry."

This recommendation was not implemented for several years after it was made.

Q All right.

I also note, Dr. Hanauer, on the next page of this report, page 18, there is a statement, and the statement of course was made in 1969, that:

"Most of the present safety research effort is directed toward providing information concerning potential accidents having very low probabilities of occurrence."

Did that direction or that emphasis continue thereafter for a number of years?

MPB/eb32

A Yes, it did, but the program was not adequate in scope or intensity so that to say "Most of the present effort" is not to imply that too much of such effort was being directed toward low-probability accidents. At this time the effort, although substantially more than zero, was inadequate in a number of respects and in particular, the LOFT program was in fact going nowhere.

However, the Semiscale program and the Separate Effects program initiated during this period provided the basis for the 1971 Interim Acceptance Criteria on emergency core cooling systems which would not have been possible without the programs initiated during this late 1960s period.

Q The next recommendation, Dr. Hanauer, is on page 21, relative emphasis on large and small accidents.

Over a decade later, I gather that's still a topic of discussion, certainly after March 28th, '79. After you've taken your time to review this section, would you care to comment on that, please, sir?

A Yes.

Q Comment on the recommendations.

A The recommendations again were considering several points of view. One of them current at that time in the development part of the Atomic Energy Commission was that the large improbable accidents should not be considered any further. This is the same issue as was discussed earlier in the discussion of quality assurance and defense in depth.

So that the first recommendation of the panel that these large accidents should remain, and the second recommendation that the large accidents should not be deleted stem from this pressure to reduce the effort in large accidents which, I remind you, at that time had not been delineated by adequate research programs.

There is also a brief comment that smaller accidents must also be included. And I must say that in view of the pressure to delete the large accidents, the emphasis in the panel's report was on retaining them.

However, on page 24 is a discussion of smaller, more probable accidents which is representative of the amount of attention they got then and for many years thereafter, they were not entirely neglected but were considered to be sufficiently easier and simpler to deal with that they didn't occupy much of our time.

Q Okay.

The next recommendation is on page 25, quantification of safety. That need was pointed out from time to time, if my recollection is correct. Shortly after March the 28th, '79, the Chairman of the ACRS or its Executive Director sent to the Commission a very brief one-paragraph letter which made essentially the same recommendation, that there is a need to better quantify safety.

MPB/eb34

But with regard to the particular recommendation of the Mangelsdorf committee, after you've refreshed your recollection, maybe you would have some comment on what the recommendation was or what progress has been made.

A This area has been transformed since 1969 by the technical activities that culminated in the Reactor Safety Study, the Lewis Report, and the Commission Policy Statement on Quantitative Risk Assessment.

One of the members of the Mangelsdorf panel believed that this type of evaluation, quantitative evaluation, was possible in 1969, but the rest of the panel strongly disagreed. And so we have recommendation one, that the risk to the public cannot now be meaningfully expressed in numerical terms, plus some merely general recommendations that work should continue in this area.

I don't believe that I interpret the recent ACRS recommendation the same way you do. As I read this recommendation, it's to take an additional step beyond the Reactor Safety Study and to establish quantitative safety goals to be used as a yardstick in the reactor licensing process which, in general, we do not now do.

So there has been a great step forward in the quantification of safety, and the ACRS has now recommended that a next large step be taken.

MR. PARLER: For the record, Dr. Hanauer's

WRB/eb35

interpretation of the ACRS letter that he has just stated was my own interpretation of that letter. I didn't express myself too well. I don't have the letter here with me.

BY MR. PARLER:

Q But I am correct that shortly after the Three Mile Island accident such a letter was sent from the ACRS to the Commission. Isn't that correct?

A That is correct.

Q Okay.

And it was a very short one, one paragraph?

A That is correct.

Q All right.

The next recommendation that I have marked, Dr. Hanauer, is on page 31, the degree of standardization and imposition of additional safety requirements, which was a matter that was receiving attention in 1969, and matters that are still receiving attention today.

Again after you've read these pages, maybe you will have some comment.

A Well, we recommended against a system of certification that was adopted some years later under Mr. Muntzing and Mr. O'Leary. So that I would have to say we were a good bit more timid about standardization than later Commissions and later Regulatory Staffs.

Q Could you comment for the record at this point on the

MPB/eb36

certification procedure, if you recall it, that was adopted by the Atomic Energy Commission in the early '60s, or is that something that you would have to refresh your recollection on?

A No, you misunderstood me. I'm speaking of the standardization policy that was adopted by the Commission and the Regulatory Staff in the early '70s, --

Q Right.

A -- about which a great deal has been written. It's embodied in the Commission's regulations.

Q Oh, yes, that I knew. I did misunderstand you but --

A My point is that this panel recommendation which is really very timid about standardization was accepted at the time, but a few years later, a completely opposite and more forward-looking standardization policy and later, standardization regulations were adopted which in fact have a number of positive approaches to standardization, which the panel did not recommend.

Q The current standardization policies, as you point out, are spelled out in regulations and in policy statements. That's how the policy evolved in the early '70s. The certification that the members of the Mangelsdorf committee was thinking about was something -- what? -- like the Federal Aviation Administration certification or --

What I'm trying to do for the record at this point is to contrast what you on the Mangelsdorf group were thinking

MPB/eb37

about as a more limited certification approach with the policy as it was eventually adopted. The policy which was eventually adopted we know about. We can look at the regulations.

What was the scope of the certification policy that the people were thinking about in the late '60s?

A We talked with the Federal Aviation Agency about how aircraft designs are certified, and I must say that the various things we were talking about in 1969 are mostly embodied in the standardization policies of 1979.

Q Okay.

The next item, Dr. Hanauer, is on page 37, criteria for deciding when to backfit after issuance of a construction permit.

After reading those pages, maybe you will comment, those two pages, 37 and 38.

A Backfitting remains a very difficult issue because we still don't have adequate quantitative methods to determine the cost-benefit equation for proposed backfits or to quantify adequately the proposed increment in safety that accompanies a backfit.

Furthermore, when we do attempt to quantify them, we find that almost never can two analysts agree on the correct values to be assigned to the components of such a calculation and that we almost always disagree with the industry about the relative benefits and relative costs.

MPB/eb38

I don't think that the panel's study and recommendation made any significant contribution to this point.

Q In other words, it was a difficult problem in 1969 and even though the regulations in 10 CFR 50.109 have been amended to say something about backfitting, from the practical standpoint backfitting remains a very difficult issue because of the reasons that you have stated for the record. Is that correct?

A That's correct. And it was the present wording of 50.109 that the panel was considering and which are being discussed in this recommendation.

Q On page 39 there's the next recommendation to involve the ACRS in the regulatory process. Perhaps what you've already said for the record and in response to my questions directed to you in your capacity as a former member of the ACRS and a former Chairman, those responses are adequate to get at what is discussed in this particular recommendation.

I don't know whether that's the case or not, but is there anything else that you could add about what the Mangelsdorf committee considered the role of the ACRS in the regulatory process should be?

A Yes. I no longer agree with these conclusions. I do not believe that the ACRS should be relieved of the obligation to review and report on all applications for power reactor construction permits and operating licenses.

MPB/eb39

I believe now, as I did not believe then, that this is an essential part of the review process. The Regulatory Staff has chosen not to take its own medicine and institute a quality control process within the Staff. We do not comply with any significant fraction of the quality assurance regulations that we have promulgated for licensees. We rely entirely or very nearly entirely on the line supervision which is essentially contrary to the principles of the quality assurance as given in our regulations.

Our only independent quality assurance with technical competence is the ACRS, since it's been shown many times that this procedure cannot be provided by the Licensing Board hearings.

Furthermore, I believe that only by participation in a large number of cases can the ACRS avoid being relegated to an ivory tower in which their considerations are so general and so divorced from reality that they don't have the necessary utility which comes, in my opinion, only from the consideration of actual cases and actual events.

This is not to say that I think the ACRS should stay out of safety issues, new data and development of criteria. I think it's absolutely essential that they be involved. And since there is only one ACRS, and I would not for a moment suggest having any more than one, and since they are part-time and have a limited resource availability, I would like to

MPB/eb40

devise a scheme whereby their participation in licensing cases was sufficiently reduced to make possible their other activity without overloading them and therefore getting poor advice.

I would therefore institute a procedure where the ACRS could decide that any given case was sufficiently like another case or sufficiently devoid of important new features that they could pass. But I do not support the proposal in this document.

Q I believe that the last recommendation of the Mangelsdorf committee is on page 42. It's entitled "Timing and Staging in Review and Decision Making Process."

On of the things that the recommendation talks about is an earlier regulatory determination than at present on the matter of site suitability. Since that time the NRC's regulations will reflect and do reflect that we have early site approval policies.

There are some other things that are covered in this recommendation. Maybe after you have looked at it you would have some comments, Dr. Hanauer.

A I don't have any comments on this. It's been overtaken by events. We now have a number of them and I don't think the process goes any better.

Q Fine.

What are the things that apparently have changed over the years from the timing standpoint with regard to ACRS

MPB/eb41

review, at least as I understand it?

Ten or so years ago it was my understanding that the ACRS -- review of the ACRS letter was narrowed to the front end of the licensing process and the Staff's Safety Evaluation came later on. And I gather now that the ACRS review occurs at a later stage in the process.

Assuming that what I have said is correct, do you have any comment on that?

A Well, what you've said does not comport at all with my recollection in the period 1965 to 1970.

Q Okay, fine.

A The timing, while not as formalized as today, was quite similar. That is to say except for extraordinary cases such as the Forst St. Vrain gas-cooled reactor, the ACRS did not seriously review a case until the Staff was finished, or almost finished.

At that time it would be possible, although it is strongly discountananced today, that the Subcommittee review of the project would take place before the Staff's Safety Evaluation had been developed. But this didn't work very well, and even in the mid-'60s, most cases were not reviewed in any seriousness until the Staff's Safety Evaluation had been developed.

MR. PARLER: Off the record.

(Discussion off the record.)

MPB/eb42

(Recess.)

MR. PARLER: Back on the record.

BY MR. PARLER:

Q Dr. Hanauer, before leaving the Mangelsdorf report, on page 38 of that report there is a reference to potential problems that might be encountered in implementing a particular criterion that the report talked about for backfitting. And one of those projects that was referred to with a potential or possibility for disagreement between the Regulatory Staff and the licensee to the safety requirements agreed upon at the construction permit stage.

:3.166

Apparently at the time of the Mangelsdorf report there was a proposed amendment to the Commission's regulations, one of the objectives of which was to minimize this problem by providing for the development and use during reactor construction of a system similar to the technical specification system presently being used during reactor operations.

This new system, according to the Mangelsdorf report, would require a delineation of the essential elements of the design and specify that these cannot be changed after issuance of the permit without prior Commission approval.

I gather that what is involved or what was involved in the effort at that time was a proposed rule to define what is meant by principal architectural and engineering criteria.

I can represent to you today that it is my

PB/eb43

understanding that such a role has never been adopted by the Commission although a proposed rule was published in April of 1969.

Now with that background, the question:

Dr. Hanauer, were you involved, as far as you can recall, in the efforts since April 1969 to provide a definition in the regulations as to what is meant by "principal architectural and engineering criteria" for the purpose of indicating what an applicant could or could not do under a construction permit without getting further Commission approval?

A I remember only that the subject was discussed.

Q But as far as you can recall, participation in any major decisions at the Staff level or the Commission level on that particular issue, you don't recall anything like that? Right?

A No, I was still on the ACRS.

Q There were efforts made after the Mangelsdorf report in 1969. As a matter of fact, the efforts by the NRC Staff in attempting to come up with a definition of "principal architectural and engineering criteria" continued through most of the decade of the '70s. But activity-- You don't recall any significant participation, --

A No.

Q -- or an awareness or understanding of what difficulties were encountered? Right?

MPB/eb44

A Well, I was probably aware of it, but I recall so little of it that it wouldn't be useful.

Q Okay.

Dr. Hanauer, I have handed you a document which I will mark for identification as Exhibit 1135.

(Whereupon, the document referred to was marked as Exhibit 1135 for identification.)

BY MR. PARLER:

Q The exhibit so marked is a letter of Dr. Stephen H. Hanauer, Technical Advisor to the Executive Director for Operation to Commissioner Gilinsky. The subject is technical issues. The date is March 13, 1975.

(Handing document to the witness.)

I have handed you a copy of the memorandum from the NRC to Commissioner Gilinsky, Dr. Hanauer. I'm going to ask you some questions about the technical issues that are covered in that memorandum. If you want to, take time to read the letter.

Shall we proceed, sir?

A Yes.

Off the record.

MR. PARLER: Off the record.

(Discussion off the record.)

MPB/eb45

MR. PARLER: Back on the record.

BY MR. PARLER:

Q This letter has in it a number of items I believe. Let's see, nine that are preceded by a title which reads "Important Technical Reactor Safety Issues Facing the Commission Now or in the Near Future."

And thereafter, under the title "Reactor Safety Policy Issues," there are four items that are talked about.

Now in the "Important Technical Reactor Safety Issues" category, Dr. Hanauer, the first one is described as design objectives and the safety design basis for water reactors.

Would you, for the record, at this point indicate what that issue is all about, issue number one?

A Well, I would really prefer to let the document stand for -- speak for itself. I believe that each one of these explains for itself, and I would rather not try to paraphrase them and have two records on the same topic.

Q That is certainly understandable, and the document will speak for itself.

But beyond that, for purposes of understanding what the root cause of some of these concerns are, I'm not too sure that the document will speak for itself on that, what the underlying causes are. Presumably there are some root causes of problems. There are some regulatory principles that are at stake, or something that led you to believe that these things

MPB/eb46

are important and, presumably, should receive attention.

Now it is my understanding after having read the item number one which will be in the record and which will speak for itself, that-- The suggestion is what? That the design-basis-accident approach in the regulations is not adequate because that is the all-or-nothing approach in the light of reality?

A That's correct. I was groping toward the same approach that the ACRS has recently proposed of using our knowledge from the Reactor Safety Study and other probabilistic approaches to modify the design-basis, all-or-nothing approach.

Q But you aren't suggesting, or you were not suggesting that the design-basis approach should be scrubbed and replaced by something else, are you, or would you?

A No, I suggested the last sentence, that:

> "Serious consideration should be given to modifying the present approach --"

which is the design-basis approach, perhaps to add some quantitative probabilistic criteria.

Q So that on that basis or with that method, the design-basis approach would be extended so that for example, instead of having 38 design-basis accidents that are analyzed and provided for, there would be, say, 60 or 70 or something like that?

A Well, I hope not. I hope it would be possible-- I

MPB/eb47

don't want to invent one at this deposition --

Q Please don't.

A -- to devise a safety review technique and technology which takes into account the things we've learned since the design-basis accident approach was devised. It served us very well, but it also has a number of important shortcomings.

An obvious example is the question of how we should factor the Three Mile Island event accident into the licensing process. One possibility is to fashion a new design basis accident out of the event sequence that occurred in Three Mile Island.

This seems to me very shortsighted because the exact sequence that occurred at Three Mile Island is only an example of a whole class of sequences which in fact were intended to be included in the design basis but in a different way. That is to say the systems and procedures were supposed to be provided to prevent the sequence from degenerating as the actual sequence at Three Mile Island did, to severe core damage.

I would like to see a scheme devised where the different possibilities of how the event sequence proceeds can be taken into account in a more realistic and probably a probabilistic way.

Q Your item number three on page two, reliability and single-failure criteria. You say that the NRC has not established quantitative reliability criteria for safety-related

MPB/eb48

systems.

And you say:

"The operating plants is one of our chief sources of information but we don't know whether the rate of abnormal occurrences now being experienced is a satisfactory one or not. We do know that nuclear units' availabilities and capacities are not satisfactory. We need to find out whether safety system availability is satisfactory, and to improve whatever aspects of reliability need improving."

That is what you have said and it will be in the record and will spea for itself.

Now what is the tie-in between reliability and single-failure criteria, again for the purpose of the record and this layman?

A The single-failure criterion is an approach to reliability requirements, grossly oversimplified, which provides a certain degree of reliability such that the failure of any single component will not fail the function of the system.

However, it is applied to systems of vastly different reliability with the result that systems complying in every respect with the single-failure criterion can have greatly different reliability, and that the specification of the single-failure criterion does not provide a well-defined level of reliability.

There are better ways of specifying reliability, but they involve uncertainties of the kind one encounters in all probabilistic calculations with the present state of the art. And it has not in general been found possible to use them in direct application to individual licensing cases.

The reason for this is quite complicated and relates to present shortcomings of the technology of making such calculations which I will describe as requiring too much art and not enough science, so that competent practitioners starting from the same information will get substantially different answers.

Q All right.

MR. PARLER: I want to mark for identification as an exhibit a Staff paper to the Commission, which I don't know whether you had anything to do with or not, Dr. Hanauer. Maybe you are not even aware of it, but I want to have it included in the record at this point as Exhibit-- I just want to have it included in the record, not at this point--

Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

It's Exhibit 1135 --

THE WITNESS: I'm sorry, 1136.

MR. PARLER: 1136.

THE WITNESS: 1135 is the Gilinsky memo.

MPB/eb50

MR. PARLER: Thank you.

(Whereupon, the document referred to was marked as Exhibit 1136 for identification.)

3.376

MR. PARLER: Exhibit 1136 is a memorandum from Edson G. Case, Acting Director, Office of Nuclear Reactor Regulation, through Lee V. Gossck to the Commissioners, subject: Single Failure Criterion, dated August 17, 1977.

478

This exhibits points out that:

"The central conclusion to be drawn from a Staff review of the single-failure criterion is that that criterion has served well in its use as a licensing review tool to assure reliable systems as one element of the defense-in-depth approach to reactor safety."

And the paper says:

"The Reactor Safety Study indicates that its use has led to a generally acceptable level of hardware redundancy in most systems important to safety. Some problems exist in specific interpretations and applications of the single-failure criterion and these are the subject of on-going work."

BY MR. PARLER:

Q Are you familiar with the Staff work in this paper,

MPB/eb51

Dr. Hanauer?

A I received a copy of the paper, and I've read it.

Q Do you know whether the on-going work that is referred to with regard to addressing problems that exist in specific interpretations and applications of the single-failure criterion, whether there's been any progress made?

A I think it's been negligible, --

Q Okay.

A -- although in the Office of Research in the Probabilistic Analysis staff there has been some method development which could, in the long run, but applicable to improving the situation.

Q Okay.

MR. SCINTO: May I ask a question at this point?

MR. PARLER: Sure.

MR. SCINTO: I just want to see the date of that memo.

THE WITNESS: Which one do you want?

MR. SCINTO: The one you just talked about.

BY MR. SCINTO:

Q In connection with the discussion you just had you indicated the progress of the single-failure criterion resolution, that there were some difficulties in that. "Negligible," as I believe you characterized it.

Are you familiar with the Commission's decision in the matter of the UCS petition relating to electrical

MPB/eb52

connectors and fire protection that was promulgated in April of 1978?

A Yes.

Q Did your comment that progress on resolving single-failure issues was negligible include consideration of the Commission's contribution, the Commission's discussion of the single-failure criterion in that decision?

A No.

Q How would you characterize the Commission's discussion of the single-failure criterion in that decision?

A I would have to re-read it.

Q Okay. That question was asked if you recall it; if you don't recall it, please don't characterize it.

Thank you.

BY MR. PARLER:

Q Back to the Exhibit --

A Off the record.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. SCINTO:

Q Dr. Hanauer, perhaps I can find a copy of it during the lunch break and you can take an opportunity to refresh your recollection in that connection.

A Yes.

MPB/eb53

MR. SCINTO: Thank you.

BY MR. PARLER:

Q Dr. Hanauer, back to Exhibit 1135, your memorandum to Commissioner Gilinsky.

On page 2 there is a discussion of human performance. Among other things you make the statement that:

"Means must be found to improve the performance of the people on whom we depend, and to improve the design of equipment so that it is less...."

You say "....independent from human performance." That word should be "dependent," shouldn't it?

A That's correct. It's a typographical error.

Q As corrected though, the complete document will be a part of the record.

I suppose a question that I would like to ask on this is apparently the matter of human performance was not given the attention certainly prior to March 28th, 1979, that it is receiving after that date; that is, human performance of those that are associated with the operation of a commercial nuclear power reactor.

A I don't agree.

Q That's the first thing: Do you agree with that?

A Human performance has received a lot of attention. Whether we succeeded in providing adequate human performance is another question which could be explored.

MPB/eb54

The technology of dealing quantitatively with human performance has not advanced very far and therefore, one would have to say that the humans made collectively a lot more mistakes affecting the Three Mile Island accident than we would have allowed for in our analysis.

I want to be clear that I'm talking not only about the operators on the scene but the people who wrote the procedures and designed the equipment that they relied on. Whether this is the result of inadequate attention to human performance is at least debatable.

It may be an inadequate technology to deal in a definitive way with human performance during accidents and transients, and that the uncertainty of human behavior is a fundamental limitation on how much can be done in this area.

Q So what you're saying is that the impression or the view that some may have that human performance was, to some considerable extent, ignored prior to March 28th, 1979, in the licensing and regulatory process is something that you take issue with. You don't agree with that. Is that right?

A Yes. I think more could and should have been done. And I'm pointing out in Exhibit 1035 that more should be done, and it's clear that the performance of humans collectively at Three Mile Island was inadequate. And to that extent our review of Three Mile Island didn't take it adequately into account, but that isn't to say it was ignored.

MPB/eb55

Q Dr. Hanauer, just for purposes of the record I would like to identify two exhibits so that they could be included in the record. I'll give you a copy of them. This is one of them.

(Document handed to the witness.)

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

The first one of these documents which I will identify for identification as Exhibit 1137 is a letter to Dr. Glen T. Seaborg dated April the 3rd, 1961, from K. S. Pitzer, who at that time was the Chairman of the General Advisory Committee.

I am including --

THE WITNESS: Off the record.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

I want to identify this document as an exhibit because even as early as 1961 -- and you will see this on the top of page two -- the Atomic Energy Commission's General Advisory Committee was considering the issue of reactor operators' examination and the need to have what Mr. Pitzer calls a reactor captain who would be in absolute charge of a facility in the same sense as a ship's captain.

MPB/eb56

(Whereupon, the document referred to was marked as Exhibit 1137 for identification.)

BY MR. PARLER:

Q Unless you have some comment on this historical document, I don't have any questions, Dr. Hanauer. As I say, I just want to have it identified for purposes of the record of this deposition. Do you have any?

A I have no comment.

Q All right.

Another document that I would like to identify for identification as Exhibit 1138 is a report to the American Physical Society by a study group on light water reactor safety dated 28 April 1975.

(Handing document to the witness.)

I have given you a copy of that document, Dr. Hanauer, which, incidentally, is not the complete report but only the summary of conclusions and major recommendations.

(Whereupon, the document referred to was marked as Exhibit 1138 for identification.)

BY MR. PARLER:

Q If you'll look at page 1-8, please, Dr. Hanauer,

PB/eb57

major recommendations of the study group on light water reactors to the American Physical Society, the first recommendation is -- and I quote:

"Human engineering of reactor controls which might significantly reduce the chance of operator errors should be improved. We also encourage the automation of more control functions and increased operator training with simulators, especially in accident simulation mode."

Now the question that I would like to ask you, Dr. Hanauer:

Are you aware of what, if any, actions the regulatory agency, that is, the Nuclear Regulatory Commission, took in response to that particular recommendation which the record should reflect was not a recommendation to the NRC but a recommendation to the American Physical Society?

A During the period of this study, in fact the simulators were coming into general use, although my first experience with reactor simulators is over 20 years ago. And the regulations were changed more or less during the period of this report to provide not only permission but emphasis on the use of simulators in the training and the requalification of reactor operators.

At some time not far from the date of this recommendation, we established an operator requalification program,

MPB/eb58

and we also made some other changes in our operator training regulations to encourage the increased use of simulators.

With respect to the human engineering I can't point to anything useful that we did. With respect to the automation of control functions, I must say that the general atmosphere around here was contrary and that in general, our licensing review process gives people a hard time when they automate control functions.

845

My personal technical opinion is that this is wrong and that functions appropriate for automation should be automated.

The whole question of division of functions between the human operator and the machine, that is to say the degree of automation, is the subject of a lot of exploration and research, not only in the nuclear power field but in such fields as aircraft and weapons, and the results are not yet entirely clear as to how much should be automated. There are differing opinions.

For example, in the nuclear Navy there is very little automation with the object of keeping the human operator on his toes. However, the direction of a weapons system such as a nuclear submarine and the direction of a nuclear power plant are really not the same problem and it shouldn't be surprising that the answers come out differently.

Q Dr. Hanauer, I don't believe that you've been asked

MPB/eb59

as yet or that you have covered it, but if you have so indicate.

How is human error considered in the application, say, of the single-failure criterion. To me as a layman, that isn't too clear. I wonder if you could comment on that.

A The answer to your specific question is it is not. The consideration of human failure comes about first from the requirement that no reliance be placed on the actions of a human operator during the initial period of a postulated event. Depending on the event, these periods vary, mostly in the range 10 to 30 minutes.

The role of a human operator as the initiator of a transient and the role of a human operator as the agent of either mitigating an accident or aggravating an accident are not explicitly dealt with in our present regulations or review practices, and this is something that has to be improved. However, it can't be done by simply waving the magic wand.

Technology will have to be developed to allow this to be done. The obvious approach is to use probabilistic techniques. But in some important areas neither the models or the data are available to put numbers on it.

Q Well, what what is the theory, that because even though what you said is the case about human error and the consideration thereof in the regulatory process, that even though it is not considered that what is required is sufficiently conservative so that one doesn't have to be

MPB/eb60

overly concerned at this time about the fact that human error is not considered in the regulatory process?

A Well, it's a technical gap in our review technology which is of concern but which we don't know how to fill without further research. And we simply have to accept whatever risk increment this entails. And many people, including myself, believe that this may in fact be the dominant, or a dominant, contributor to the actual risk posed by nuclear power plants today.

The Safety Study and vai us studies since that time have shown that something between one-third and two-thirds of the risk involves human failings of one sort or another.

Q That's the Rasmussen Report that you're referring to, WASH-1400? Is that right?

A Yes.

Q On page three of your memorandum to Commissioner Gilinsky, item number seven is entitled "Degree of Detail and Realism in Safety Evaluations." Again, everything that you have said there will speak for itself, but in the interest of possible clarification or enlightenment, is the suggestion in seven essentially the same as the suggestion in number one?

It would appear to me -- in your number one -- it would appear to me to be the same, but I have a feeling that they are not because otherwise you wouldn't have had a number one and a number seven.

MPB/eb61

A No, they're quite different. Number one dealt with the requirements, the design objectives, the safety goals, and the substance of the review.

Q Right.

A Number seven deals more with the methods.

Q Right. Ckay.

A The substance of the review requires the analysis of certain sequences of events, in the present scheme the design-basis accidents. But in any scheme there will have to be analysis of the course of some sequence.

What I am suggesting here is that as we get better and better codes we can analyze in fact a whole lot more than we want to know; that we have to decide how much we need.

What I didn't suggest here and what I would say today if I were going to discuss the subject is a need I perceive much more than I did in 1975 for getting rid of what I then called the broad-brush treatment with plenty of arbitrary conservatisms.

This is embalmed in such evaluation models as the one specified for emergency core cooling. The difficulty is whether the arbitrary conservatisms in the analysis lead to a result which is so unrealistic that it is useful only for the sequence and region of parameters for which it was derived.

You can learn, for example, almost nothing from such

MPB/eb62

a calculation about the real safety advantage of making changes in the system because the calculation is so arbitrary and so divorced from reality; the result is that an approach of this sort which I was, to some extent, advocating then I do not advocate today, will in fact give you the wrong answer.

It will tell you that a certain change is in the direction of increased safety whereas a more realistic calculation or experiment will tell you just the opposite. This has greatly impeded, in the period since 1975, all efforts to put into our emergency core cooling calculations the results of the theoretical and experimental research that the taxpayer has spent so many hundreds of millions on in the last few years.

I think this is a major shortcoming of the present approach which had to be adopted at the time it was adopted because that's all we knew, and the state of mind which persists after the state of technology has changed has in fact inhibited both safety improvements and improvements in realism and economy.

So I feel rather differently about this one than I did four years ago.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. PARLER:

MPB/eb63

Q On page four under "Fuel Performance" in the concluding sentence you state:

> "Related technology of establishing fuel damage limits under accident conditions is even less established...."

than what you referred to earlier in that paragraph --

> "....principally because PBF...."

which I guess is the Power Burst Facility --

> "....is so many years late."

Has any progress been made in that area since 1975?

A Yes, but I can't say it's in very good shape. The Power Burst Facility is now operating. We have a good bit of experimental information.

On the other hand, it is still true that we continue to find fuel damage phenomena in normal operation and in transients. The pellet-clad interaction phenomenon is still not well understood. We've just finished a series of discussions about what would be the correct fuel damage limit to use in analyzing anticipated transients without scram. And neither the industry nor our own Staff was able to propose anything that realistically modelled the damage phenomena or a realistically derived damage threshold. So that this area is still not in a satisfactory state.

134

Q All right.

A Let me say that it's possible to impose conservative

PB/eb64

damage limits, but these result in a very large, unnecessary cost to the public in some cases.

Q Moving to the second part of your memorandum to Commissioner Gilinsky under the title "Reactor Safety Policy Issues," the first one there is internal quality assurance.

I believe you have already spoken, perhaps in another context this morning for the record that the policies are expressed in Appendix B to Part 50, the need for quality assurance on licensees and others, but that policy or the equivalent thereof is not applied to the NRC organization.

That is the point that you are making here under number one -- right? -- that we don't have any internal quality assurance requirements that would be applied to the regulatory process, to the quality of our organization? Isn't that your point, Dr. Hanauer?

A I think that's what I said earlier in discussing the role of the ACRS.

Q Right.

Now a number of others in the intervniews that we've had have made essentially the same point, technical reviewers, for example. And the question I have is:

Do you know whether anyone has made any effort to get something done in this area, in other words, to call what appears to be a concern to the attention of the Commissioners and make recommendations to them?

MPB/eb65

A Well, this paragraph is typical of the needles I have applied in various quarters over the years, but in fact nothing has happened.

Q Okay.

Now the next item raises, as I understand it, the matter of the generic decisions. The title is "Making Better, Faster, and More Generic Decisions."

Is my understanding correct that what you're talking about primarily is the so-called generic lists of unresolved safety issues, or is something broader than that involved here?

A Well, no such list existed back in 1975.

Q Fine.

A I must say, however, that my optimism in 1975 about ATWS was not justified and that neither of my examples has yet been resolved four years later.

What I was talking about was the inordinate time and effort to decide anything outside the licensing case. It was fashionable then and it is fashionable today to attempt to resolve issues generically which, in its dictionary sense, means applying the same resolution to a number of different, in this case, licensing cases but which around here means sweeping it under the rug and not including a resolution of this issue on a particular case on which it has occurred.

The fiction is preserved-- That's too strong. The policy is preserved that some resolution must be obtained on

MPB/eb66

each case of all significant safety issues, but all too often, the so-called resolution is only that when we finally get around to deciding the issue this decision will be imposed on the particular case under consideration.

Sometimes we do in fact decide the issue and impose a decision upon the case in which it was raised. In many others-- In this case, the system has worked correctly and the issue was decided generically, which is a great economy because you don't want to try and resolve the same issue in ten different cases by ten different reviewers and maybe in ten different forums.

In far too many cases, however, even when the issue was resolved it simply joined the backlog of application to all but new cases and remains unresolved in the sense that whatever has been decided has not in fact been applied to modify the actual plant systems.

In many other cases these issues have hung around for years and years and decisions have not been made. The recent actions by NRC management to the Technical Activities Steering Committee have made some progress.

I was recently appointed Director of Unresolved Safety Issues by the NRC and so my job is to take the most urgent and important of these issues and make progress on them.

An important element of progress that I can take no credit for was the study of all 130 generic issues then

MPB/eb67

outstanding, first on the basis of their reactor safety and public risk potential, and then a broader study of a number of factors including the most important one, being the effect on safety and risk which resulted in a priority ranking of these 130 issues.

The top 20, including the 19 unresolved safety issues so designated by the Commission, and issue B6, load combinations which I discussed earlier, were given top priority and I have been given resources with which it is scheduled and foreseen that these will be resolved in a reasonably timely way; that is to say almost all of them within the next year or a little more.

The second batch of about 25 were targeted for contract work but in general, manpower within the Staff was not available to do more than follow the contract work, and so the resolution of these issues will in general be postponed for a number of years, although some few of them are actually coming to fruition because of the urgency of the decision in some particular licensing arena.

The remaining 80 or so issues have third priority and I have to say that many of these will in fact never receive the kind of attention that the top two groups will receive. I think this is all right, and in fact as part of the Commission's consideration of this question, about a year ago each one of these issues that is not going to be worked on was considered and a rationale and technical basis were established why this was okay.

My own opinion is that any issue you can leave around for several years without working on, you might as well forget about. If it's all right to let it go five or ten years then it's all right to let it go forever. This is an opinion not universally shared, and it may be that some of these will be promoted, either by improved understanding or by events.

I would expect that and it has been anticipated by Mr. Denton and Dr. Mattson that the lessons learned from the Three Mile Island accident will result in a number of additional unresolved safety issues being promoted to high priority and experience in operation research results in improved understanding from regulatory considerations will provide a trickle of new issues that need prompt and some rather intensive treatment.

MR. PARLER: Mr. Lanning, did you have some questions?

BY MR. LANNING:

Q Prior to your current position as Director of Unresolved Safety Issues, were you previously involved in the Staff response or review of the technical issues identified in NUREG-0138 and 153?

A Only peripherally in that I provided advice to the Executive Director for Operations when the Commission papers came through his office.

Q Did the Office of EDO review or comment on the NUREG reports?

A Not formally, although there was some discussion.

Q Did you attend ACRS meetings concerning the discussions of these technical issues?

A Some-- That's not a useful record. Some of them.

Q Do you recall whether or not any of these ACRS meetings that you attended included a discussion of issue four identified in NUREG-0138 as the loss of offsite power subsequent to manual safety injection reset following a LOCA?

A No, I can't recall whether I was at that discussion. I'm familiar with the issue and have been in discussions of it.

Q These are discussions prior to the Three Mile Island accident?

A Yes.

Q There are at least two examples of attempts to include in this technical issue the analyses of the loss-of-coolant accident assuming interruption of ECCS at any time during the accident.

MR. LANNING: We should identify these two exhibits.

MR. PARLER: That would be 1130.

Do you have copies for Dr. Hanauer?

MR. LANNING: Yes.

The first one we will identify is Exhibit 1139, a

MPB/eb70

memorandum from Mr. Marinos to Ben C. Rusche. The subject is "Resolution of Technical Issues," dated November 19, 1976.

(Document handed to the witness.)

The second exhibit we will identify is 1140, which is an excerpt from the hearings before the Committee on Government Operations, United States Senate, 94th Congress, Second Session, dated December 13, 1976. And it's starting on page 260 through page 262.

(Whereupon, the documents referred to were marked as Exhibits 1139 and 1140 for identification.)

MR. PARLER: Let Dr. Hanauer read those, please, before you ask him questions.

(The witness reading.)

4.341

BY MR. LANNING:

Q In these discussions you had on this particular technical issue, had they included the consideration of interruption of ECCS at any time during the assumed LOCA?

A That's the issue.

Q The issue as stated in NUREG-0138, that is pretty narrowly defined and limited to Westinghouse plants. The Exhibit 1139 commented on the description of the technical issue and suggested that it be expanded to include the analyses of the LOCA considering interruption of ECCS at any time.

mpbl
flws
eb70

And the Staff response in NUREG-0138 really doesn't address the issue from the broader sense of analyzing LOCAs considering prolonged interruption of ECCS.

My question is: Has the Staff considered the results assuming the interruption of ECCS during, for example, the design basis LOCA?

A Not explicitly. The Staff assumes, and I've always assumed, that a sufficiently severe interruption of off site power or a large number of other functions during the course of a large loss of coolant accident would melt the core.

Q Therefore, since the consequences are so severe, any variations of interruption of ECCS to more define the allowable limits for interruption of ECCS was never considered?

A Well, the issue, as you suggest, is poorly stated both by Mr. Marinos and by the Staff document. I'd like to suggest that a correct statement of the issue would go something like this:

In considering the requirements for protection against loss of coolant accidents, which sequences involving degraded performance or availability of protection functions should be included. If you consider the sequence of events which begins with a large pipe rupture, there are in fact an extraordinarily large number of possibilities. The Reactor Safety Study, after eliminating the ones which were not physically possible and those which were believed to be a very

mpb2

low probability, ended up with 43 event sequences all starting with the large loss of coolant accident. And it is possible to conceive of a large additional number, although they were analyzed in the Reactor Safety Study not to constitute significant risks.

Only one of these sequences is the one required to be considered in the regulations, 10 CFR 50.46 and 10 CFR 50 Appendix K. This required sequence includes a number of failures of safety related systems. Among them are the hypothesis that all offsite power is lost, and the hypothesis of the occurrence of the most severe single failure in the equipment which remains.

In most plants and for most analyses this most severe sample failure is an additional failure of a diesel generator set providing the energy for the emergency core cooling system. Now it is easy enough to postulate the occurrence of additional failures during the course of a loss of coolant accident, and Mr. Marinos and others have made proposals along these lines. The basic reason that the Staff has not accepted these proposals is the belief,which was not well quantified when originally expressed,that these sequences involving additional failures were sufficiently improbable compared to the ones that were considered that the risk increment was not very large.

The discussion in the NUREG reports you refer to

mpb3

was an attempt, not especially successful, to show that this was true for the particular sequences proposed by Mr. Marinos. It is possible to pursue this line of thought essentially indefinitely, and a principal contribution of the Reactor Safety Study is the organization of thought along these lines made possible by the techniques of event trees and fault trees, so that the 43 event sequences I referred to earlier are the 43 branches which survive on an event tree which originally contains several hundred potential branches.

Q How has human error been included in the single failure criteria as applied to implementation of Appendix K?

A As far as the single failure criterion is concerned, human error is not included. Human error is accounted for to some extent by the requirements that the initiation of the emergency core cooling system and its necessary auxiliary functions be automatic and not rely in any way on human action; and by the requirement that the transition from the injection phase to the recirculation phase required in large accidents be automated.

However there is, as I said before, no explicit account in the analysis of other possible human errors, of omission or comission, or of human actions which might mitigate the accident. Both are omitted from the analysis.

Q Concerning the loss of offsite power during the assumed accident, Exhibit 1140 included an ACRS recommendation

mpb4

that the loss of offsite power at any time subsequent to the occurrence of a LOCA should be studied further by the Staff.

Are you aware of any activities that followed up this ACRS recommendation?

A I would, please, like you to point out the part of this exhibit you're talking about.

Q On page 262, the last paragraph.

MR. PARLER: Give Dr. Hanauer time to read it, and then maybe he'll want you to restate the question.

(The witness reading.)

THE WITNESS: I just don't know whether an additional study along these lines has been made. There are several generic issues dealing in one way or another with the loss of offsite power, the reliability of the offsite power system.

One of them is Unresolved Safety Issue A44, which deals with station blackout, a more severe system in which both offsite and onsite power are lost. Another is Generic Issue A25, dealing with the reliability of offsite power. And I frankly don't know whether that or some other study is directly responsive to this or not.

I could have a look and provide additional information for the record if this is desired.

MR. PARLER: Why don't you do that. And then at the time you send back your transcript corrections, that will

mpb5

be a convenient time, perhaps, for you to say what you found as a result of your look-see. If you found something, include it; if you didn't find anything, say that you didn't find anything.

bu5

Is that all that you have?

Have you got anything on generic items righ. now?

MR. COX: No.

MR. PARLER: Off the record.

(Discussion off the record.)

(Whereupon, at 12:00 noon, the deposition in the above-entitled matter was recessed, to reconvene at 12:45 p.m., this same day.)

mpbl

#5/bu5

AFTERNOON SESSION

(12:45 p.m.)

MR. PARLER: On the record.

Whereupon,

STEPHEN H. HANAUER

resumed the stand as a witness, and, having been previously duly sworn, was examined and testified further as follows:

MR. PARLER: You had a question, Mr. Cox, that you would like to ask Dr. Hanauer?

MR. COX: Yes.

EXAMINATION (Continued)

BY MR. COX:

Q Dr. Hanauer, it's my understanding that the design of most nuclear power plants now operating or under construction are such that the control room operator can significantly decrease ECCS flow, maybe even terminate it --

A That's my understanding also.

Q I haven't finished yet.

A Sorry.

Q -- at any time after this ECCS flow is automatically initiated. That is your understanding?

A Yes.

Q Do you feel that this is a necessary feature of reactor plant design?

A Yes. I don't think it's possible to foresee

mpb2

enough of the combinations of events to have thought out in advance and automated all possible actions in the control room during the course of an accident.

Instead what we've done is to automate the initial response and to rely in substantial measure on the operator. In a large number of events that have occurred this was justified.

In the Three Mile Island accident the operator, abetted, as I said, by the people who designed this equipment and wrote his procedures, made a substantial number of significant mistakes which exascerbated the accident.

I don't think it's possible to decide in advance that this, that or the other action should be made impossible for the operator to execute because in most cases not very much thought will suggest to you alternative courses of events in which the action would be adviseable or even required. These systems are sufficiently complex, and the variety of sequences which can be foreseen but sometimes are not foreseen is so broad that after an initial automated response one has to rely on the general programming of the computer which is the human brain, because of our present inability to program an electrical computer to do the same thinking function.

What I'm saying is that as an event actually unfolds there is no substitute for human thought in deciding the correct course of action. With this, one has to accept

mpb3

a probability, hopefully fairly small, that incorrect courses of action will be chosen, and that the accident will in fact be initiated or worsened by the actions which were allowed by the reliance on the human operator that I've described. And this occurred in Three Mile Island and in other events also.

I don't know of any way to make an important improvement. One would, if not careful to discover that one was always, like the French Army, deciding for the next previous battle or the next previous event. The next event, for example, might occur in such a way that it's important to shut off the high pressure injection pumps, for instance, to prevent overpressurizing the primary system and causing a loss of coolant accident, which of course is what the operators erroneously thought they were doing.

But sometimes it isn't an error. And I don't think we are at a state of knowledge where all these sequences can be predicted. And I think it is, therefore, a risk we have to run to provide the means to turn off the emergency core cooling system.

The defense against it is primarily well-educated, well-trained, intelligent operators who have the knowledge and experience to do the right thing, and the temperament to apply their knowledge and experience at times of stress. They should be aided by a good set of procedures and a good set of equipment which maximizes their knowledge of conditions

mpb4

in the plant and their understanding of it.

Q That's all I have.

BY MR. PARLER:

Q The current status of the generic unresolved issues, is that set forth in the report this year to the Congress, or is there a more current list that you're using as a working document?

A There is a more current list. It just came out. I will identify it as NUREG-0606, Volume 1, number 1. It's dated September 4, 1979, known as the AQUA Book, A-Q-U-A, in which is set forth for each unresolved safety issue a network of milestones and schedules together with a summary of the problem description and the current status.

Q Is that your only copy?

A It's the only one I have. It's freely available from MPA on the payment of a modest sum.

Q All right.

THE WITNESS: Off the record.

(Discussion off the record.)

THE WITNESS: On the record.

BY MR. PARLER:

Q You mentioned earlier before our recess the delays, the long time span over which it takes to get attention and action going on generic issues. Certainly that appears to be the case prior to March 28, '79, and prior to your assumption

mpb5

of your current position.

Generally speaking, to what do you attribute that? Is it resources, for example, or what?

A My own opinion is that the primary cause is the resolution of generic issues was not given a high enough priority to get it done.

Q Who had the responsibility for the resolution of generic issues prior to the assumption of your present position?

A It was widely dispersed. The principal was effective about two years ago. Each generic issue was assigned to a cognizant supervisor, usually an assistant director. Before that the responsibility was even more diffuse.

Q Some have suggested that a part of the situation leading in the past to the lack of proper attention to generic issues may be the vague language in which the need for some of these issues has been advanced by others such as the Advisory Committee on Reactor Safeguards.

Does that contribute to the problem?

A I don't think so. I think that the issues have a wide spectrum of need and urgency and therefore priority. For each Class A or Class B issue there is a problem description which seems to me sufficiently specific that the problem you suggest is not a major factor.

Q There are some who have suggested that if an issue which might be a generic issue is raised by a presiding

mpb6

licensing board in a licensing proceeding, that such an issue receives prompt regulatory staff attention, as contrasted to, say, for example, a generic issue that might be raised by the ACRS, which receives less than prompt attention, for example.

Do you have any comment on that?

A I would broaden the comment, which is generally true, that any issue which requires resolution in the context of an individual case finds some kind of resolution on a schedule more or less consistent with the schedule of the case, that to delay a licensing proceeding for ten years to resolve some particular issue -- and the resolution of some issues has occupied ten years -- would be intolerable, and that therefore those issues which must be resolved in order to move a licensing decision forward get the top priority.

I think this is just the way people work.

Q In other words, it's a practical reality of the licensing process which one should not conclude, because of that practical reality, that the staff is engaging in either unintended or some other procrastination regarding ACRS generic concerns.

See, the appearance to some is since the response in the licensing arena is prompt and not so prompt in the other arena that there is some sort of a, oh, not significant attention being given to the concerns of the Advisory Committee on Reactor Safeguards.

mpb7

A Well, I think that's a misplaced inference, that the ACRS itself decides this issue by either requiring that the issue be resolved in the context of the case before they issue their statutory report or by themselves deciding that the issue can be deferred for generic consideration.

Once the decision is made that it's all right to defer an issue, it's natural that procrastination sets in. This happens for deferred issues from whatever source.

Q What role does the regulatory requirements review committee play in the generic issues area? What I don't understand is how that committee interfaces with the technical activity steering committee.

A The technical activities steering committee is primarily a management function. They approve test descriptions, task action plans. They establish priorities, or, to be more precise, they advise the director of the Office of Nuclear Reactor Regulation and the Commission regarding priorities.

They review progress. They review and approve or not proposed changes in scope or schedule.

The regulatory requirements review committee deals with the products. That is to say, the regulatory requirements that come from the consideration of the generic issues. The resolution of a generic issue is typically embodied in a NUREG report, often incorporating or referring to one or a large number of technical reports from the industry, from NRC

mpb8

research, from technical assistance and other technical resources, and embodies the Staff recommendation signed out by the division director of the resolution of the issue.

Now since the issue is almost always in the form of what shall be the requirements related to some technical area, the resolution is a proposed set of requirements. In some cases the general aspect of these requirements will already have been established either by regulation, by guide, or by some other action which, if it came in at the right time frame, was already reviewed by the regulatory requirements review committee. In other cases new ground is broken and new requirements are proposed, and in that case the requirements are in general reviewed by the regulatory requirements review committee.

The question of the details of this process, when and how public comment should be obtained and so on, we're still learning by experience.

Q After something, for example, say, a regulatory guide is presented to the regulatory requirements review committee and that committee makes a decision, that guide should be placed in Category Three, which for purposes of that committee, that is the regulatory requirements review committee, means to me that the area that is involved should be backfitted, who is responsible for implementing that decision in the organization, do you know?

mpb9

A The regulatory requirements review committee was established by the Executive Director for Operations, and in the final analysis reports to him. The committee decisions are transmitted to the officer responsible for the action; in the case of Standards and Guides to Mr. Minoke; in the case of Standard Review Plans and Branch Technical Positions, to Mr. Denton.

If these officials agree with the decisions of the committee, they say so and order the implementation by whatever the correct organization is. If they don't agree or if there's disagreement among the officers, Mr. Gossick provides the resolution. And in principle, although it's never happened, this could be appealed to the Commission.

Q Were you involved, in your prior duties, with the implementation of Regulatory Guide 1.97, I believe, instrumentation to monitor the course of an accident?

A Not directly. I knew about it as advisor to the Executive Director for Operations.

Q Now apparently that is an area where the generic work had been done, the regulatory requirements review committee had made its decision about what category that guide should be placed in.

I gather that the subject matter is off of the unresolved safety item list, and then there is a question of having it implemented, is that right?

mpb10

A That's my understanding.

Q But other than what you've already said, you don't have any insights into the major problems that have been encountered in implementing that guide, or do you?

A I don't have any direct knowledge, and I don't want to speculate.

Q All right.

A I know that there is an effort now underway as part of lessons learned to finally do something about that subject.

Q All right.

MR. PARLER: I would like to mark for identification and for purposes of the record two exhibits. The first one will be Exhibit 1141 which is a letter from Mitchell Rogovin, R-o-g-o-v-i-n, director, NRC TMI Special Inquiry Group, to Dr. Max Carbon, Chairman, Advisory Committee on Reactor Safeguards. The letter is dated June 29, 1979.

In that letter Mr. Rogovin asked the ACRS a number of questions.

(Whereupon, the document referred to was marked as Exhibit number 1141 for identification.)

MR. PARLER: Off the record.

(Discussion off the record.)

mpb11

MR. PARLER: On the record.

And the reply from Chairman Carbon to Mr. Rogovin, dated July 25, 1979, I will mark as Exhibit 1142.

(Whereupon, the document referred to was marked as Exhibit number 1142 for identification.)

BY MR. PARLER:

Q Of course, Dr. Hanauer, you haven't seen these letters before, and I should mention to you I'm not going to ask you any questions about them. I want them placed in the record because in Exhibit 1142 Dr. Carbon -- or Chairman Carbon, in his reply, states in part that the Committee, that is the Advisory Committee on Reactor Safeguards, feels that the response of the NRC and of the AEC before it in connection with -- quote -- "instrumentation to follow the course of an accident" -- close quote -- has not been adequate.

Although this item has been addressed by the issuance of a regulatory guide, that guide has not to the Committee's knowledge yet been implemented on any operating nuclear power plant.

And, continuing, Chairman Carbon says:

"Although the NRC has given increased attention and resources to the so called "unresolved generic items" within the past

mpb12

two years, we would welcome additional emphasis on resolution of these items."

The response of Chairman Carbon also has an attachment to it which, among other things, bears generally on some of the broad items that I asked Dr. Hanauer questions about at the outset of this deposition, regarding concerns in certain areas that have been expressed by the Advisory Committee on Reactor Safeguards in past years.

Off the record.

(Discussion off the record.)

MR. PARLER: On the record.

BY MR. PARLER:

Q We're still under the broad category of your letter of March 13, 1975, to Commissioner Gilinsky, and I wonder what your comments would be on the following -- and I ask this question in the context of your item number three under Reactor Safety Policy Issues, Stabilization of Regulatory Requirements and Standardization of Design.

In view of the variety of customized designs that apparently exist in the industry, it would seem to this layman at least that it would be very difficult to achieve what I think of as an integrated or irrational national safety regulatory policy. Are the two related or not?

A Well, you'd have to define your terms better. There were too many buzz words in it. Rational national safety

mpb13

policy issue, what do you mean?

Q Well, if you had, for example, 24 auxiliary feedwater systems -- which I understand you have -- maybe just for pressurized water reactors -- how can the people in the Nuclear Regulatory Commission who write the standards and the criteria write standards and criteria that would deal with those things, how can the people that sit in this building and elsewhere go about reviewing the vast variety of things?

Those are the underlying thoughts that replace the buzz words.

Now with that replacement, do you have any comment?

A Yes, I do.

Q Please do so.

A The way in which a regulator copes with a variety of designs --

Q Right.

A -- is to distill the essence which is the safety performance or the safety significance from them. And so for feedwater systems, for example, certain principles have been ennunciated and the requirement is that the state water systems comply with those principles, and then if necessary, design by design and plant by plant to review their compliance with these principles.

This is laborious. It would be a lot simpler for us if there were one auxiliary feedwater design for all

mpb14

plants. It would still be necessary for us to decide what was required of an auxiliary feedwater system in order to make a proper decision on whether this single design was adequate or not, although in a large number of cases -- particularly during the earlier days of this regulatory program -- we performed a review of these systems without having explicit requirements, and this was based on a kind of an instinct that this design was satisfactory without an articulated basis.

A whole lot of correct decisions were made, but it was pretty hard to see the basis for them without an articulated set of basic safety requirements.

What standardization would save us is the necessity to review each design and to determine whether or not it complies with the safety requirements.

MR. PARLER: Did you want to ask questions about the regulatory requirements? I think the context is probably right.

BY MR. LANNING:

Q Have you ever been a member of the Regulatory Requirements Review Committee?

A I was a non-voting observer representing the Executive Director for Operations from the time the Committee was formed, in about 1973, until last December when I left the Office of the Executive Director for Operations.

Q What was your purpose in that capacity?

A The Director of Regulation and the Executive Director for Operations never articulated why they wanted me on there.

(Laughter.)

I define my own position in the following way:

First, I maintained a cognizance of what was going on in the Committee and reported to the Director of Regulation or to the Executive Director for Operations the problems that might come to his attention or that I thought should come to his attention in the operation of the Committee, both procedural and technical. I also had not the slightest hesitation and was in fact encouraged to state my own technical views on the various subjects that came before the Committee.

MR. PARLER: Mr. Cox, go ahead.

BY MR. COX:

Q I have a question on standardization again, Dr. Hanauer.

Again, based on your long experience and history as technical advisor at the highest management levels for the NRC, the NRC has been pursuing a development and implementation of standardization policies for several years now, and as you brought out earlier, they have many policy statements in that area, and we even have regulations, I believe, Appendix O and several other appendices to 10 CFR 50.

Do you feel -- or perhaps let me ask it this way:

mpb16

What are your feelings, opinions, comments, whatever you care to offer, about the viability of the program now in light of TMI-2? Are we at a standstill? Are we able to move as planned before? Are there changes necessary?

A I don't think they have anything to do with each other. Standardization is a method for approving designs or portions of designs in advance so that the review of individual cases can proceed in a more economical and expeditious way.

When new technical questions arise from Three Mile Island or anything else, they have to factor into the process. If as a result of Three Mile Island a large number of new questions or new requirements arise, as seems likely, then all reactors, standardized or not, will have to be rereviewed, and all previous approvals, standardized or not, will have to be reconsidered.

The biggest impact of Three Mile Island on the standardization process is that if there are no new applications, standardization seems rather meaningless.

Q You mentioned expedition and economy. Do you feel that standardization, per se, has any safety advantages to be gained?

A I think there are potential safety advantages to standardization. In principle it allows much larger resources to be applied to the safety design and the safety review for a much smaller number of designs. I have not yet seen any

mpb17

evidence that this is in fact taking place.

Q Increased safety or a smaller number of designs?

A Either one.

MR. PARLER: Are you finished?

MR. COX: Yes.

BY MR. PARLER:

Q Your last item in this memorandum to Commissioner Gilinsky talks about "too many surprises", and without going over what you've already said there, it is my impression that one of the areas in which it has been recognized that prior to March 28, '79, there was room for improvement in the regulatory area was the area of the systemmatic review and operation of operating information, operational feedback information.

Now it is also my understanding that the Commission has recently approved the creation of a new group, the Office of Operational Data Analysis and Evaluation, or words to that effect.

Do you believe that such an office could minimize the -- quote -- "too many surprises" -- unquote -- that you refer to in your memorandum to Commissioner Gilinsky, or is that too broad a question for you?

A It's not too broad a question; and the answer is no. I think the new approach is likely to improve the agency's response to surprises. But I don't see how it would minimize the number of them.

mpb18

Q I realize -- and I believe I am correct -- that that office, although it has been approved, it has not yet been established. Is that your understanding?

A I'm not up on this sort of thing. I know Mr. Heltemes, H-e-l-t-e-m-e-s, has been appointed either acting director or interim director of that office.

Q Fine.

The point that I was going to get to is this:

Is it your understanding that the office of -- that we've been talking of -- Operational Data and Analysis Group, that it would just make recommendations, or would it have other authority?

A It's not clear --

Q Okay.

A -- from any of the pieces of paper I've seen how much clout it's going to have.

My experience is not hopeful that the fractionation of this function into six groups in six separate offices does not give me any comfort.

Q Now incidentally, were you involved in your official capacity or otherwise in the insights that went into the creation of this office? Did anybody ask for your views?

A No, sir, although they were provided to the Executive Director of Operation over a year ago. I would like to put into the record a memorandum I wrote on that subject,

mpb19

which I will have to get and retrieve from the files.

Q Would you please do so.

Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

Dr. Hanauer has someone looking for the document that he just referred to.

BY MR. PARLER:

Q Do you recall enough about the document so that you can describe it, Dr. Hanauer?

A It was a general survey of the necessity for and the present arrangements for feeding back new information into the licensing process. This new information can arise not only from operating informat on but from research results and from improved insights during the licensing process.

In particular with respect to operating information, I concluded that it was everybody's business and therefore nobody's business, and recommended some improvements. No response was ever made.

Q When that document is available I will mark it for identification and put it as an exhibit to this deposition.

A Off the record.

(Discussion off the record.)

MR. PARLER: On the record.

The document will be marked for identification at

mpb20

this point in the record as Exhibit 1143.

(Whereupon, the document referred to was marked as Exhibit number 1143 for identification.)

MR. PARLER: When it is made available I will give whatever additional description is required.

Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. PARLER:

Q Dr. Hanauer, we've just been talking about one limited aspect of a recent organizational change and how it bears on what you were talking about in your memorandum to Commissioner Gilinsky, "too many surprises".

Now what other comments would you have on the subject of why "too many surprises"? You obviously felt in 1975 that there were, and presumably there are some reasons for that,and may be some areas in which actions can be taken to, without eliminating it, eliminating them, maybe reducing "too many surprises".

Please comment.

A I don't think the number of surprises is under our control. I think the rate at which surprises come are a measure of the maturity of the technology and of the industry,

mpb21

and that in mature technologies the surprises come at a much lower rate.

We have had in the last year again too many surprises. We've had the seismic shutdowns, we've had Three Mile Island, we've had more concern with environmental qualification.

This tells me that the technological maturity, so strongly put forward by industry representatives, has not yet been attained. As I said, I don't think there's anything the NRC can do about this. But it's part of an inevitable learning process with a new technology, and that we simply have to develop the fortitude to receive these surprises and effective means of dealing with them when they come, and to be willing to accept the implications not only of what these surprises contain one by one, but the rate at which they occur.

MR. PARLER: The document that we were referring to earlier and marked for identification as Exhibit 1143 is a memorandum from Dr. Stephen H. Hanauer, then technical advisor to the Executive Director for Operations, to Mr. Lee V. Gossick, Subject: Feedback of Information into the Reactor Regulation Process, April 26, 1978 is the date, previously marked as Exhibit 1143.

BY MR. LANNING:

Q I'd like to ask you a question on the topic we've

mpb22

just been discussing about "too many surprises".

The exhibit references a discussion of that issue, Item 3 in the paper which is entitled Stabilization of Regulation Requirements and Standardization of Designs. It's not clear to me what the relationship is of how we would respond to surprises and the stabilization of regulatory requirements.

A A certain fraction of the surprises are evidence that the requirements aren't right and have to be changed, the other fraction being evidence that plants thought to be in compliance with the requirements are in fact not in compliance. To the extent that the requirements elicit changed -- I'm sorry. To the extent that the surprises elicit changes in requirements, the process is not stabilized and standardization has to be changed in accordance with the new requirements. And that's the connection.

MR. PARLER: Anything else?

MR. LANNING: No.

BY MR. PARLER:

Q Dr. Hanauer, before leaving Exhibit 1135 -- which is what we've been talking about for the last hour or so -- I would like to show you an article which you co-authored I guess in 1971, and the purpose of this is just a couple of paragraphs that are on page 207.

MR. PARLER: We'll mark this article for

mpb23

identification as Exhibit 1144.

(Whereupon, the document referred to was marked as Exhibit number 1144 for identification.)

BY MR. PARLER:

Q This is an article by Dr. Stephen H. Hanauer and Dr. Peter A. Morris, Technical Issues on Large Nuclear Power Plants.

I gather that this paper was presented at -- what? -- the International Atomic Energy Agency, or do you recall, Dr. Hanauer? I don't --

A This paper was presented at the International Conference on Peaceful Uses of Atomic Energy in 1971.

Q All right.

Having so identified the document, would you turn to page 207, and the two paragraphs in the middle of the page starting with "The principal defense against accidents", that paragraph and the next paragraph.

After you've read them I want to ask you some questions.

(The witness reading document.)

c6

Q Now I ask you to look at the language in the 1971 article in the context of what you said in your memorandum in 1975 to Commissioner Gilinsky under Item One, Design

mpb24

Objectives and Safety Design Basis for Water Reactors.

There in your memorandum to Commissioner Gilinsky I believe, if my recollection is correct, you refer to the more realistic viewpoint of a spectrum of accidents, each with probabilities and consequences of its own. And I wonder if you're thinking in your memorandum to Commissioner Gilinsky about design objectives.

Is that consistent with what you said in your 1971 article -- and the purpose of this is to make certain that all of your insights in this area about design objectives and design basis accidents are as clear as they can be for purposes of this record.

A I think the comparison of these two references shows the progression of my thinking. Reference 1044 in 1971 describes the approach that I characterize in Exhibit 1135 as the "all or nothing approach".

Q Right.

A By 1975 I had become somewhat less enchanted with this approach and recommended that we look for alternatives.

Q Okay.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: On the record.

BY MR. PARLER:

Q This 1135, your memorandum to Commissioner Gilinsky,

mpb25

although it may be self-explanatory from your covering letter of transmittal to the Commissioner, what was the occasion for this memorandum? Did the Commissioner ask you to provide it or what?

A He called me up and asked me for such an appraisal.

Q What was his response to your memorandum, do you know?

A I never received any.

Q Have you been asked for a similar appraisal by any other commissioners?

A No.

Q So this type of memorandum, a response to a request from a commissioner asking for your candid appraisal of regulatory policy issues, reactor safety issues, to the best of your recollection is the only one of its kind in what has been referred to on past occasions as the "Dr. Hanauer Nugget File" is that correct?

A No, sir. This has no connection whatever to the "Nugget File".

Q It does not?

A None whatever.

Q Would you clarify that for me, please, because I thought that's how I located this document.

A You did not.

Q Okay.

mpb26

A The "Nugget File" is a file I have kept for many years of events which for one reason or another I wanted to preserve for my future use. In recent years it consists mostly of licensee event reports. In earlier times this was not as well organized, and so the entries before about 1970 are from a variety of sources, almost all of them in the public domain.

Q Righ t.

A A "nugget" being a piece of gold in a much larger pile of base material not worth saving. There are several thousand LERs a year, and I save perhaps 50.

Q And I believe you covered what you're talking about now to some considerable extent in your deposition before the President's Commission, is that right?

A That's correct.

Q Now wherever I located this document, the Exhibit 1035, whether in your files or anywhere else, as far as you're aware that's the only document of its kind that you have produced, is that right, that is to a commissioner on broad reactor policy questions, reactor safety questions.

A That's correct.

Q Fine.

#[illegible] (6.068)

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. PARLER:

mpb27

Q Dr. Hanauer, I've handed you a memorandum from yourself as Assistant Director for Plant Systems, Division of Safety Systems, to seven individuals who are the addressees. The addressees are indicated on the first page of your memorandum. The subject is, one, environmental qualification, two, instrumentation to follow the course of an accident. The memorandum is dated April 6, 1979.

MR. PARLER: I'll mark it for identification as Exhibit 1145.

(Whereupon, the document referred to was marked as Exhibit number 1145 for identification.)

BY MR. PARLER:

Q Now, Dr. Hanauer, my understanding as a layman of this memorandum, it is that after -- and indeed this was shortly after April 6th -- the Three Mile Island accident experience, you had some additional thoughts about regulatory matters. These are set forth in your memorandum.

Now to the extent that these thoughts are of significance from the standpoint of either broad regulatory policy matters or regulatory matters that are important to safety, I would like for you to comment on this memorandum.

I realize, again, that the memorandum speaks for itself, but -- with the insights that you had that you were

mpb28

trying to call to people's attention and have them explore -- would you comment on that, please?

A   Well, first I'd like to characterize the memorandum differently.

The addressees are the people on the second page in the list marked "Addressees".

Q   That's right.

A   The seven names on the first page received copies. The addressees are people who work for me or people directly in my business.

Q   That's a good question, by the way. Thank you.

A   The people on the first page are my colleagues and bosses.

The paper must be viewed as an early reaction. I think it's correct today. But I wouldn't like to characterize it as my technical reaction to Three Mile Island. It's only a small part of it.

The two subjects are related. That is to ay, we were in the throws of losing some of the instrumentation, primarily the pressurizer level indication that we were using to maintain the plant shut down in its interim condition. And this elicited these thoughts about what ought to be qualified for what kinds of accidents.

Since I was talking about instrumentation, this naturally led to the subject you've already alluded to, namely

mpb29

instrumentation following the course of an accident, which, as you point out and as the ACRS pointed out, has not yet been applied on any reactor.

I think this is really a fairly small part of the lessons to be learned from Three Mile Island. It's necessary. There is now a special study going on under Mr. Wenzinger, W-e-n-z-i-n-g-e-r, to revise not only Reg Guide 1.97, but the other regulatory guidance in this area.

I think that in thinking over the implications of the Three Mile Island accident we have to divide the reactions into two parts. There are, first of all -- or into several parts -- there are, first of all, the various kinds of failures and mistakes which contributed to the accident, which contain a substantial amount of information not previously available and which should be used to improve the design process and the regulatory process. This is primarily a technical problem exemplified by some of the hardware recommendations of the lessons learned task force.

Then one can take a somewhat broader view and use these technical items as examples of whole areas in which the design and review process was inadequate, one obvious example being the area of environmental qualification and instrumentation to follow the course of an accident, in which there were some notable shortcomings. And so we say not just that the pressurizer level instruments need to be qualified, but that the whole idea of what has to be qualified for what kinds of accidents and what information the operator needs as he guides a plant through some kind of a severe accident has to be rethought.

Then on still a higher level of abstraction, one has to consider whether, as has been discussed in this deposition already, whether the whole idea of a series of design basis accidents against which protection has to be provided as essentially the sole basis of the safety design of the plant is in fact the satisfactory one. And I've already made a number of comments on that.

Q Right.

A Finally, at the ultimate level of abstraction is the question of whether the whole process of private independent design, construction and operation of nuclear power plants designed either one at a time or a few at a time in a proliferation of so called standard designs reviewed one at a time or a few at a time by a government agency with a few hundred or a few thousand people, depending on how you reckon them, supported by a research program of the present dimensions is in fact an adequate enterprise, and whether the public wants it to be continued, let down or expanded, and whether this should be redirected in some substantial way or whether the present approach is adequate.

On this last point I'd like to make one observation.

mpb31

If one thinks back a few years one can discern on the order of once a year events with varying consequences to the public, but which have the common characteristic of making the nuclear industry and the Nuclear Regulatory Commission look like a bunch of idiots. Examples are the Browns Ferry fire, the environmental qualification petition by the Union of Concerned Scientists and the events that led up to it, the inadequacies in the seismic evaluation of plants which led to five plants being shut down, and the Three Mile Island accident.

There are other examples that come to mind. And so something like once a year one might legitimately question whether the people responsible for nuclear reactor safety know what they're doing.

Two possible answers at opposite ends of the spectrum suggest themselves. The first one is that such a rate of discovery that the nuclear enterprise is conducted by a bunch of idiots is not tolerable and that a very large improvement is required to protect public safety and to give the public the necessary confidence that safety is being maintained.

At the other end of the spectrum would be a conclusion that these are complicated machines, that a large number of people are involved, that people are going to continue to make mistakes, and that the acceptability of nuclear power depends on whether or not about once a year it

mpb32

is satisfactory for the people who are responsible for nuclear safety to look like idiots.

I believe that a case could be made for either of these responses, or in fact both, but that the first one, if true, means that we shouldn't have nuclear power. I think it would take an enormous effort to reduce the incident rate of such -- I'm searching for a word -- perceptions of failure by a factor of two and that the public would hardly notice that the rate had been decreased by a factor of two.

To decrease the lead by a larger factor I think is probably impossible, and therefore I tend toward the second answer, that the conduct of this or any other comparable enterprise will be accompanied by failures and mistakes, that machines are imperfect and people make mistakes, and that this is inevitable.

We have designed our plants with a great deal of that overworked cliche "defense in depth" so as to be resistent to the consequences of a lot of mistakes and a lot of equipment failures. Three Mile Island shows us that such failures and mistakes can pile up to the extent that the plant is essentially ruined. It can also be argued that Three Mile Island shows us that even a ruined plant with a large release of fission products from the core didn't hurt anybody much.

I think the country will have to decide whether accidents like Three Mile Island are in fact intolerable, in which case I suspect that the operation of nuclear power plants is intolerable. We can add six more lines of defense and protect against the Three Mile Island sequence, but I don't think we can protect against all possible sequences with a degree of assurance a whole lot better than the one we now have.

I really do think that we ought to do our business better, and I think ways can and should be devised to do them. But I don't think this will be the end of our making mistakes.

Q Dr. Hanauer, from a narrower regulatory perspective than the broad TMI implications that you've just covered, I wonder,in the area of safety related equipment,if you have any thoughts on that. You pointed out in the document which has been marked as Exhibit 1145 you're relying heavily on things not defined as safety related. You say that Browns Ferry was like that too.

And I suppose in connection with TMI that one could ask whether the PORV manual control system should have been classified as safety related? There seems to be from other representations that we have received some uncertainty in that area as to where the regulatory process should go.

Do you have any comments on that?

A I'm not much impressed with the importance of your specific question, whether the PORV should be classed as safety related or not. I think the question is important in an

mpb34

entirely different context, namely that whether the PORV is safety related or not, its malfunction contributed substantially to a severe accident.

Q Right.

A And it is also used to mitigate event sequences which in this particular class of reactors can become severe accidents.

This tells me that another previous dichotomy between safety systems, which we spend a lot of effort on, and non-safety systems, on which we spend essentially zero effort, is not a correct approach, and that a more graduated approach is needed where equipment in the gray area between safety related and non-safety related, such as the power operated relief valve, should get its proper attention.

Q I was going to ask you this question from the perspective of a layman:

Although one might not be impressed with the PORV relief valve example that was given as not being safety related, is my understanding correct that if a piece of equipment or a system is deemed by the regulatory process to be safety related that that means that at least theoretically that it receives greater attention in the regulatory process and therefore one could believe that it would have a -- be more likely to work than to fail?

A Well, you have in fact understated it.

mpb35

Q Okay.

A Almost the entire attention of the regulatory process is directly exclusively at safety related equipment. Only for such equipment, with minor exceptions, are there any requirements at all. And such equipment is in general required to be of very high quality.

Q What are the minor exceptions, if you've finished, if you recall them?

A Well, I'll have to think a minute.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: On the record.

THE WITNESS: Well, one exception -- which is not a very good example, for reasons I'll tell you in a minute -- is the reactor control system. The reactor control system is not safety related and has in fact been sorely neglected, but at least not completely neglected, and to that extent is an exception to the general rule that I stated earlier.

In fact, I believe now that the previous neglect of that system should be rectified, and that it should get its proportionate share of attention based on its potential to induce accidents if it malfunctions, and to contribute to the accident's response if it functions correctly.

Q Why isn't the integrated control system, or the control system -- you said it was not completely neglected

mpb36

even though it's not safety related equipment.

Now for the record, could you indicate why, even though that system is not safety related equipment, it is nevertheless not completely neglected?

A I think it's only tradition, the idea that the control of the nuclear reactor was important and difficult, which is not true, and some vestage of that concern still can be seen in the non-zero attention the system got.

Q What I'm trying to get to is this, Dr. Hanauer:

It's my understanding that even though the control system is not considered by the regulatory organization as being safety related for the reason that you just stated again, that nevertheless in some respects it is treated as if it were safety related.

Now what I'm trying to get at is in what respects is the control system treated as if it were safety related? Maybe I misunderstood your earlier testimony.

A I hope I didn't say that because I didn't intend to say it. The control system is not treated as safety related but it gets a degree of regulatory attention in making sure that its failure would not create or aggrevate an accident outside the reactor safety design basis.

MR. PARLER: Mr. Scinto, did you want to ask something?

MR. SCINTO: Let's go off the record for a minute.

mpb37

(Discussion off the record.)

MR. SCINTO: On the record.

THE WITNESS: In thus discussing the reactor control systems I distinguish it from the reactor protection system which shuts down the nuclear chain reaction and, as required, initiates engineered safety features, which are of course a part of the safety design basis of the plant and are reviewed in detail as part of the regulatory process.

MR. PARLER: Mr. Lanning.

BY MR. LANNING:

Q How does the NRC distinguish between which equipment is safety grade and which equipment is non-safety grade?

A The short answer is that safety related equipment has to be safety grade. That doesn't say anything.

The requirements are principally set forth in the Standard Review Plan, although some of the most important ones are in the general design criteria. The Standard Review Plans set forth in considerable detail which systems are safety related and what the requirements are for them, which you abbreviate by saying "safety grade".

Q Is there a definition in the regulations or used in practice by the Staff for defining "safety related"?

A There is a definition for "safety related equipment". I can't, from memory, tell you where it is.

There is not a definition anywhere for "safety grade".

mpb38

It's a form of shorthand. For electrical equipment it usually means conforming to a group of standards headed by IEEE 279 and 603.

For pressure retaining components it means designed in accordance with an appropriate section of the ASME boiler-pressure vessel code Section 3. For other kinds of components the definitions are different.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

Dr. Hanauer, while we were off the record, remarked that the exhibits that were previously marked for identification only as Exhibit 1137, Exhibit 1141 and Exhibit 1142, that he would prefer that they not be included in the record of his deposition even though only marked for identification. His point was that since he was not questioned on these exhibits and did not have an opportunity to express any views at all, he would prefer that these exhibits which I have just referred to not be bound with the record of his deposition.

The binding of these exhibits in the deposition was primarily for the purpose of administrative convenience, since it has been known that from time to time we are evicted because of weather conditions from our premisis. However, even though that is the case, I find that Dr. Hanauer's request is entirely reasonable and therefore the list of

mpb39

exhibits that are identified at the outset of this deposition shall not include Exhibits 1137, 1141 and 1142, nor should these three exhibits be bound in the record of the deposition.

THE WITNESS: Thank you.

(Whereupon, the documents previously identified as Exhibits 1137, 1141 and 1142 were WITHDRAWN.)

MR. PA^LER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. PARLER:

Q Dr. Hanauer, I hand you a document which I will mark for identification as Exhibit 1146.

(Whereupon, the document referred to was marked as Exhibit number 1146 for identification.)

This is a document from Harold R. Denton to Robert B. Minogue, dated July 12, 1979. The subject is Instrumentation to Assess Nuclear Power Plant Conditions During and Following an Accident.

Is this subject something that you have been involved in in recent months?

A Peripherally. I attended the meeting on July 3rd,

mpb40

1979, referred to in the second paragraph of this memorandum.

Q I gather that the substance of this memorandum is to try to work something out so that there can be a joint effort between NRR and Standards in trying to get the Regulatory Guide 1.97 implemented, is that correct?

A That's correct. The ACRS pointed out correctly that this guide had not been implemented.In its review of the Three Mile Island accident the Lessons Learned Task Force decided that prompt action was needed in this area and felt that a special group should undertake it rather than diverting the limited resources of the task force itself.

The result was the meeting described between Dr. Mattson, head of the Lessons Learned Task Force, and representatives of Nuclear Reactor Regulation and Standards Development offices, in which the decisions summarized in Mr. Denton's memo were taken.

Q In your long experience in the regulatory area as the technical advisor to the Director of Regulation, and then to the Executive Director for Operations, is the way that this issue is being handled, that is at the office level, typical of the way that major problems that would require resources of more than one office are coordinated and handled?

A Yes, this often happens. In fact it has been institutionalized between Nuclear Reactor Regulation and Research in the form of formalized user needs, and between

mpb41

Standards Development and Nuclear Reactor Regulation in the form of standards initiation forms, which are concurred in by office directors.

Q Suppose that one of the -- or the office director that the memorandum is directed to of the Director of Standards Development would have had some higher priority? How does the organization come to grips with that? I'm asking you that question, not necessarily from the standpoint of your current position, but from the perspective that you gained during your years as the technical advisor to the Executive Director for Operation and to his predecessor?

A Memos like this are almost always preceded by informal contacts.

Q What do you mean, things that were sent in advance and then the memorandum is written?

A The memorandum then formalizes agreements already reached in almost every case.

Q Suppose agreements cannot be reached between the principal office director's concern, what then happens?

A Then it has to be considered by the Executive Director for Operations or the Commission.

Q In your experience were there frequent occasions under which there had to be resolutions at those levels, that is at either the EDO level or the Commission level?

A No, but it's not unknown.

mpb42

Q It's not unknown.

So this Exhibit 1146 from your experience would be a typical approach in the organization for the resources of more than one office to be mustered to handle a high priority item, is that right?

A Yes.

Q All right, thank you.

MR. PARLER: Now I will mark for identification -- go ahead, Mr. Lanning.

BY MR. LANNING:

Q In your memorandum to Mr. Gossick, identified as Exhibit 1143, in the recommendations section on page 5, number three states:

"Put a time limit on how long NRR can delay an IE circular or bulletin."

Do you have knowledge of examples where I&E bulletins have been delayed by NRR?

A Yes. I can't be specific, it was too long ago. But in my investigation of the feedback of operating information, the IE circular or bulletin was one important way in which operating information developed in one plant or one incident was fed back to the other operating units for their information or action.

And there was a series of incidents in which draft circulars or bulletins had been sent to NRR for

mpb43

concurrence and had been delayed by many weeks.

Q Do you remember either the subject or the time frame of these delays?

A The memo was written in April, 1978. It would be in the months preceding that.

Q Do you know of any subsequent discussions between Mr. Gossick and NRR and I&E office directors to resolve this or to implement the recommendations?

A No.

MR. PARLER: Do you have any other questions?

MR. LANNING: No.

BY MR. PARLER:

Q Dr. Hanauer, I'm going to mark for identification as Exhibit 1147 what has been represented to me to be comments by Admiral H. G. Rickover, U.S. Director, Naval Nuclear Propulsion Program, in a meeting with members of the President's Commission on the accident at Three Mile Island.

The Admiral's comments are dated three-quarters down from the top of the first pages with the date July 23, 1979. That is the date of his comments, as far as I am aware.

(Whereupon, the document referred to was marked as Exhibit number 1147 for identification.)

I gather, Dr. Hanauer, that --

mpb44

A Do you want to give it a number?

Q Yes, 1147.

You've never seen or read that document before, is that correct?

A That is correct.

Q Adm. Rickover in this document, which I will certainly give you the time to read, starting on page 6, it talks about basic principles of the Naval reactors program. And then later on he discusses other principles which he believes are important.

In other words, he talks about the basic principles for the Naval nuclear propulsion program, and then later on he gives ideas of what principles in his judgment would be sound principles for commercial nuclear power programs.

I would like to try at least, after you have screened this document, to refer certain things to you to ask you to comment on. In a number of these areas it would be my understanding that the material that is involved is in the same area of the kinds of things that you've already discussed in the context of questions that were asked about the Mangelsdorf report and also questions that were asked about your memorandum of March 13, 1975, to Commissioner Gilinsky.

If you would prefer, however, not to proceed on this route, we will not proceed on this route.

mpb45

A Well, I don't mind. I acquired a great respect for Adm. Rickover in my review of Naval reactors while a member of the ACRS. I have been scanning this, and it is consistent of what I know of his actual operation.

Q All right.

MR. PARLER: Let me go off the record for a second.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. PARLER:

Q We will start on page 23 of the Admiral's suggested actions, and the Admiral comments that, in his first suggested action, that:

"Utility management, as the owners and operators of the plant, have prime responsibility for their safety."

There are a number of factors that are involved in the construction and operation of a nuclear power plant, the vendors and the architect-engineers. All the utilities are licensed.

It would appear to this layman at least that the vendors and the architect-engineers play a very important role, although they are not licensed. And at least as far as the architect-engineer is concerned, the architect-engineer would appear not to be too heavily impacted by the regulatory process.

mpb46

Now I gather that what the Admiral is saying, that the utility management as the owners and the operators of plants have prime responsibility for their safety, that that principle is reflected in the Nuclear Regulatory Commission's regulatory approach to the licensing and regulation of commercial nuclear power plants; is that your understanding?

A That's my understanding. And the principle is, of course, embodied in our basic structure and our rules, and even in the Atomic Energy Act. In almost the same breath I have to say that whereas utility management, when asked, will invariably say the right words about their contentions regarding this responsibility, and the architect-engineers and vendors and others will state the correct things about their responsibilities for safety as agents or suppliers to the utility, it's my experience that some decisions are made on the basis that safety is what the Nuclear Regulatory Commission requires. And in some areas some utilities do not make any independent judgments about the safety of their plants.

bu7

I think that Adm. Rickover is correct, and that the attitude that I just described is not correct, an inimical to safety.

Q Is there anything of which you are aware in the regulatory process which would encourage or provide any incentives to utilities that are licensed to operate nuclear

mpb47

power plants to go beyond the minimum requirements of the NRC, the minimum regulatory requirements? What are the incentives?

A There are no incentives in the regulatory process since the requirements are all we can impose. The incentives would be the decreased risk for the company and the public.

Most industry people, including most utility people, honestly believe that since the NRC is way over-conservative in their requirements anyway the risk to the company and the public is already negligible and nothing beyond the minimum NRC requirements are justified.

Q Would you say that the regulatory process to some extent at least may indeed inhibit innovations in the interest of safety?

A I'll go further. I think the regulatory process strongly inhibits innovation.

Q What is there in the regulatory process that --

A Let me say one thing in answer to the preceding question.

Q Go ahead, please.

A I'd like to point out that the standardization policy and the standardization process is an even stronger inhibition on innovation. This has positive and negative aspects.

MR. PARLER: Off the record.

(Discussion off the record.)

mpb48

MR. PARLER: On the record.

BY MR. PARLER:

Q Dr. Hanauer, would you please elaborate on the record what those positive and negative aspects are?

A The positive aspects are the desire to standardize the designs and to restrict changes of all kinds, including innovations,in favor of stabilization of the designs, of the safety design basis, of our understanding of the machines, and of the similarity of the many machines that we have to deal with.

This is in fact the basis for the standardization policy.

The negative aspect is that such of these innovations that are in fact improvements in safety are equally inhibited.

Q All right.

MR. SCINTO: I've got a follow-on, if you'll let me, Bill.

MR. PARLER: Go ahead and ask it.

BY MR. SCINTO:

Q Dr. Hanauer, I've sometimes heard the standardization policy characterized as in fact standardizing only the NRC regulatory review and not in fact standardizing the designs of the plants subject to that review.

Could you comment on that?

mpb49

A Well, if it's true, this wouldn't be standardization at all. The reason -- Let me go back.

The standardization policy of the Commission and the Commission regulations related to the standardization clearly envisage standardization of designs. Standardization of review, economization of review and elimination of repetitious review makes sense only if the designs of the plants themselves are standardized.

BY MR. PARLER:

Q Moving over to page 27, please, of this exhibit, Item number three, Adm. Rickover says:

"There should be a government representative in the control room at all times with the authority to shut the plant down if he believes this to be necessary for safety."

If this is an area you have an interest in or a point of view on, would you care to comment? If not, then we'll proceed.

A Yes. I worked for years with an operating organization at Oak Ridge. I think the increment of safety provided by this is very small, that almost all of our bad accidents happen to plants that were nominally shut down, or plants that were in fact shut down without any difficulty as far as the immediate shutdown was concerned and then got into trouble one way or another.

mpb50

In the Three Mile Island plant, for example, the decision to shut down was an automatic one caused by the scram being initiated. And there would, in fact, have been no difference in the Three Mile Island event had Adm. Rickover's recommendation been taken.

A more serious possibility in my opinion would be the potential for an independent representative -- for example, a government employee -- in providing an independent and somewhat detached point of view in a degraded situation. It's difficult to speculate whether Adm. Rickover's government representative might have had a clearer insight as to the incorrect actions and the incorrect inferences which were drawn by the operators in the Three Mile Island control room, whether he could have pointed out the trend of the plant toward saturation in the primary system and the other less obvious mistakes in evaluating the situation which were made by the operating people.

I think that the Lessons Learned Task Force recommendations for improved control room manning addressed this question in a more direct way, and I'm not inclined to favor Adm. Rickover's suggestion.

Q Briefly, what is the more direct way that the Lessons Learned Task Force approached the thing, without going into detail?

A It relates to the command provisions and to the

mpb51

establishment of the technical advisor position in the control room to be manned around-the-clock.

Q Would that be an advisor who is an engineering graduate, a nuclear engineer or something?

A Yes. I'll refer you to the Lessons Learned report, which I don't want to characterize.

Q I was not asking you, Dr. Hanauer, to characterize it, or I did not intend to. But I want to get to this question:

I gather from what you have said that it may well be that under circumstances such as TMI-2 that the presence of the government representative may not have made a difference. Is my understanding of what you said correct?

A Well, I was speculating on whether it might have made a difference, and it just might have. But the fact that he was there with authority to shut the plant down I felt was rather irrelevant.

The plant shut itself down and then got into big trouble.

Q Well, if you would have somebody in the plant who was not a government representative with authority to shut the plant down, but a nuclear engineer who had had some experience, would you speculation be the same?

A Well, that's the recommendation of the Lessons Learned Task Force, which I endorse.

mpb52

Q All right.

Item number four in Adm. Rickover's list is that:

"All activities involved with nuclear power, utilities, reactor vendors, manufacturers and regulatory agencies must establish and attain as permanent a staff as possible as long as they perform well."

Is there anything in the regulations that you are aware of or in our regulatory policies that addresses itself to this point?

A No. This is almost a cliche. As far as the regulatory -- I'm on page 28 of the same reference, now.

"To retain people, they must be paid adequately. More important, to attract and retain good technical people, they must be trained and given authority and responsibility. Nothing causes technical people to leave more quickly than not being able to do their technical jobs properly."

And so on.

These are almost cliches. They are, of course, correct. The regulatory program does not address these sorts of things. Many of the regulatory policies are viewed by plant personnel, designers, architect-engineers, as making their jobs less attractive. They are always subject to quality

mpb53

assurance inspectors peaking over their shoulder. They get their operator licenses jeopardized.

And I don't know what to do with your question except to remark that regulatory necessities sometimes work against this.

Q Well, let me help you with what to do with the question. Let's move away from the cliche part, if you will, Dr. Hanauer, back to what I thought was the fundamental point that was being made, and that is that there is something to say for having qualified people around for some period of time and not have a continuing transfer of people from one place to another, have a head or a chairman of the plant operations review committee for three months and then another one for the next three months, et cetera; have one unit superintendent for several months and then another one.

The stability of people in key positions, the qualifications of people that are in those positions, is that something that our regulatory process gets involved in as far as you are aware?

A Not at all, as far as I am aware.

Q All right. That's the question.

The next question is: Should it, in your judgement?

A I don't offhand see how. It's a highly desirable state of affairs that I don't see how to promote in a regulatory fashion.

mpb54

#7

Q The next item that Adm. Rickover talks about, plant design, control room training, and so forth, should be standardized insofar as practical. In this discussion today you've addressed yourself to standardization on several occasions. Perhaps there's nothing else to add here. Is that right?

A That's what I think.

7.171

Q Now on page 29, Adm. Rickover says:

"Minimize reliance on automation and computer control."

And I don't know whether what he says here is inconsistent with what you said earlier or not. If you would care to comment on this?

It certainly is, by the way, just as a comment, and as the Admiral points out, his recommendation or his thinking here runs counter to the belief of some others, which may not include you.

A It does.

What he stated is a desired effect which may or may not be capable of achievement. The plant, he suggests, should be designed and built in a simple stable fashion, but that's not always possible, nor is it true necessarily of Naval facilities either.

Furthermore, for routine control and management tasks it would seem better to me to program a machine, computer,

mpb55

if you like, to do the things which are best done by a machine, and leave for the human operator those things which are done better by humans than by machines.

This is an old argument.

Q About the point that is made about the bottom of page 30, it says:

"An inherently stable reactor makes fewer demands on the control systems and the operators. Therefore it results in a simply more reliable plant, et cetera."

In the context of the Babcock and Wilcox design, and prior to the bulletins and orders, corrections, after March 28, 1979, do you have any thoughts on the extent to which the sensitivity of a reactor should be a factor in the regulatory process?

I don't know whether I'm communicating clearly the question or not. It's a question of a layman --

A Yes, you are.

Q Okay.

A Yes, I think so, and I've suggested informally that we really don't know enough to quantify sensitivity and to decide how much sensitivity is too much.

It's clear that the Babcock design reacts more quickly and overshoots more violently than the other two current pressurized water reactor designs. It's not clear

mpb56

that this makes it unsatisfactory, but only by comparison to the others it has a more difficult control problem. This is why the Babcock and Wilcox integrated contro l system was devised in order to provide for the plant and its control system a more stable and less sensitive response.

Q The Admiral's export item number seven, which is on page 31, Dr. Hanauer is:

"Simplify and reduce the size of the control rooms."

I don't know whether you have any comment on that or not. Do you, sir?

A Yes. I used to design control rooms for a living.

The control room at Three Mile Island and most other control rooms in nuclear pow . plants now in operation could have been designed by my colleagues and me in the early 19 0s. They make no use, or very nearly no use of any improvements in hardware of understanding acquired since that time.

They are built without adequate consideration of the limitations of the human body or the human brain. And I believe that it's very important to improve the design of control rooms to the extent that I think it will be found appropriate to require the backfitting of almost all the existing control rooms.

We have now a new generation of control rooms,

mpb57

starting at the Susquehanna Plant, where the man-machine interface is managed in an entirely different way through the use of a computer interface and cathode ray tubes.

One of the most attractive features of this control room is that we don't know yet what the problems are, and our early experience with the new control room designs I predict will be just terrible until we shake them down.

Furthermore, the data presentation, information presentation to the operator and the utilization of the potential of a computer interface is in fact rudamentary and even childish in its early designs, which is not surprising. It's a little like trying to use the first big digital computers before we had invented FORTRAN and other languages to address them.

The machines were ludicrously better than the capability of the people to use them. This is going to be true of the new control rooms, and I would therefore not jump up today and require that all plants be backfitted with them.

However, after a period of experience in which I trust that some altogether new and now unforeseen methods comparable to the development of FORTRAN in digital computer programming will be developed to communicate these data from the plant to the operator. I think it will become appropriate to backfit improved control rooms in all plants.

I'd like to say one more thing.

mpb58

Q Go ahead.

A On the bottom of page 31 and the top of page 32 a report by the Electric Power Research Institute is identified.

Q Yes.

A This report itemizes in devastating length and detail the shortcomings of a number of control rooms identical in concept and similar in design to the one at Three Mile Island.

As far as I know, no action has been taken to ameliorate the worst aspects of these control rooms in existing plants.

Q The situation that you have alluded to in your answer, or in your comment, at this point as well as earlier, the lack of progress in the area of control room design, do you attribute that to the influence of the experience that the utilities have had with the fossil plants?

A Partly.

Q Partly, to the lack of what? Regulatory push --

A Utilities, there are a number of reasons for it. In the first place utilities are very conservative technically. In the second place, they got sold a very bad bill of goods. They -- right after World War II they bought a bunch of vacuum tube control equipment which had a terrible availability record, and it cost them a large amount of money in decreased plant availability.

mpb59

Q You're talking about fossil plants now?

A Yes. There weren't any nuclear plants right after World War II.

To this must be added the generally regressive nature of the Nuclear Regulatory Commission review, particularly in this area, which is in general inimical to improvements and treats them with a very large number of negative questions and positions, even when there is an obvious safety improvement involved.

I blush to admit that that branch is under my supervision or was for some period of time.

Q Which one is that?

A Instrumentation and Controls.

Q I see.

Speaking of instrumentation and controls, Adm. Rickover's point number nine refers, at the bottom of page 32, to instrumentation matters, direct reading instruments, et cetera. I don't know whether there is anything in that discussion that you want to comment on, or even if you've had time to reflect on what the Admiral said.

A I'm just scanning it. It seems eminently sensible to me.

Q All right.

Well, I suppose, at the bottom of page 35, item eleven, at least for purposes of the record I should ask you

mpb60

to comment on the Admiral's point that:

"Do not succumb to calls for more research and development as a response to the Three Mile Island incident."

You should take time to read what he has said on that page and at the top of the next page. And if you'd care to comment, I'd appreciate it.

(The witness reading.)

A I agree completely. I have in fact seen, both inside and outside the government, very large research proposals based nominally on Three Mile Island.

Q Is that all you have to say about that, sir?

A Yes, sir.

Q All right.

Let me move back, if you don't mind, or turn back to page 10A.

This page covers some of the principles that the Admiral follows for nuclear power propulsion programs. I'm talking about the second item from the top there. That's what I'm going to refer to.

He says:

"Design, build, operate and maintain the plant so as to prevent accidents rather than relying on systems and procedures provided to cope with accidents after they occur."

mpb61

It would appear to me as a layman, Dr. Hanauer, that perhaps the regulatory approach of the Nuclear Regulatory Commission is just the reverse. It's concerned with the mitigation of accidents after they happen. To me as a layman that is the essence of the design basis accident approach.

Would you please comment and correct me if I'm wrong?

A Yes. This was widely misunderstood, although not by Adm. Rickover.

In principle, we subscribe completely to the first part of that sentence and it's one of the echelons of defense. And as the Manglesdorf panel pointed out, it is in fact the most important of the echelons of defense.

If I were building weapons that had to fly or swim or go under the sea, I might take the emphasis that the Admiral gives. If I'm building nuclear power plants with thermal power in the 3- to 4000 megawatt range, I would like to have an additional echelon of defense, which he tends to deprecate, namely, I want the machine built, designed, operated and maintained so as to prevent accidents. And then I want it acknowledged that the designing, building, operation and maintenance of these plants will be less than perfect, that equipment will fail, people will make mistakes. And I want systems and procedures provided to cope with accidents after they occur in addition.

mpb62

Now maybe I can't cram all of that onto a submarine, but I can put it on a nuclear power plant, and I want both.

My point is that whereas in other in other designs one may have to choose, I don't think we do in nuclear power plants.

Q It's clear from what you have said that in the commercial nuclear power area that the emphasis should be placed on both preventing accidents as well as mitigating the effects of accidents if the accident has happened.

A I believe strongly that this is the case.

Q Okay.

Now where is the -- other than quality assurance, how does the regulatory program, that is the NRC, emphasize the provisional aspect? Would you pursue that a little bit more, please -- Let me make one other statement.

There are some inspectors in the field that have represented to us that when there is an immediate safety problem that they have encountered, they don't have any problem at all receiving attention from headquarters. But if there is something that is preventive in nature, at least in their judgment, they have great difficulty, or at least some of them have experienced great difficulty in getting people to pay attention to their concerns.

Those examples may or may not be correct, but that

mpb63

is one of the reasons why I am asking you for your views as to how, beyond quality assurance, the regulatory process deals with, emphasizes the preventive aspects.

A Our primary reliance, aside from the quality assurance program, with the preventive aspects has been all in the fact that it is to the utilities' self-interest to design, build, operate and maintain the plants so as to prevent accidents which involve down-time.

I think consistent with their discussion of control systems, for example, which are to prevent accidents, I think we have probably overdone it and that we probably have to pay more attention to preventive devices of which control systems are an example.

Q Okay.

Moving back to the area of the generic items, it's my understanding -- and perhaps you testified earlier -- that the original list of some 133 items have been or has been reduced to 19, with the addition of -- what? -- the B6 item that I believe you referred to.

There are some who may believe that this reduction may have come about in large measure because of the definition of unresolved safety item that someone came up with in the past.

Do you care to comment on that?

A Well, I don't think you've characterized very well

mpb64

the description I gave of the process which you characterize as reduction.

The situation was such that it seemed obvious that all 130 items did not have equal priority, and that there weren't enough resources to get them all done promptly.

Q Right.

A And therefore there was a prioritization.

The definition and concoction of the term "unresolved safety issue" was in fact done by Congress in a clause in the authorization bill a couple of years ago. The Commission's definition of an "unresolved safety issue" was given as a response to that. It was devised by the Staff and approved by the Commission.

The unresolved safety issues are therefore those of the generic items which have the highest priority which are the most serious or potentially serious to safety which involve more than one plant and which have at least the potential for being unsatisfactory in their present state for the lives of the plant.

Q Right.

A Now I'm not sure I understand your question in that context.

Q Incidentally, just for the clarification of the record, I was not in my question characterizing your early testimony. My point was that some have represented -- some,

mpb65

not me -- have represented that one of the reasons why the long list of 133 could have been reduced to the 19 was because of a vague definition of unresolved safety items or allegedly vague definition of unresolved safety items which could mean different things to different people.

I have gathered, and it's my understanding from what you have said just now a minute or so ago, as well as earlier in this deposition, that such in your judgement is not the case, that the priorities that we now have are indeed based on what sound analysis which has resulted in an identification of those things which are of the greatest importance to the safety of nuclear power reactors.

Is that what --

A Yes, I described that process in earlier testimony.

Q Okay.

MR. LANNING: I have a question.

BY MR. LANNING:

Q As part of the Technical Activities Steering Committee, it's my understanding that a group of individuals reported to that committee to prioritize the generic issues by considering each issue and assigning a point value based on some guidance. And it is this technique which resulted in the prioritization of the generic issues.

Is this the process that you're referring to as being properly quantified as to the safety of the issue?

mpb66

A As I testified earlier, the process actually went in three steps, of which you have described the second.

The first step was a study by the probabilistic analysis staff of the risk potential in each one of the issues. And this resulted in an evaluation for each one, of the impact on public health and safety of resolving the issue. This was one of the inputs to the process which you have described, and was in fact the largest contributor to the point rating which also considered other factors, requests from the ACRS, promises that were made to somebody, efficiency of the regulatory process, environmental effects and other things.

This was all reviewed by the Technical Activities Steering Committee, and in the case of the unresolved safety issues, by the Commission. And the result is the priority values that I described.

MR. SCINTO: I'd like to clarify the time.

MR. PARLER: Go ahead.

BY MR. SCINTO:

Q In this review, the one in which you have indicated the Commission was involved, was that -- do you have in mind when we're talking about that review, the review in which the Commission overrode the recommendation by Mr. Denton with respect to at least one issue, and that was on system interactions?

A That's correct.

mpb67

Q Okay.

A It took place about a year ago.

Q Right.

If I mischaracterized it, change that. I'm just trying to identify the timing.

A That's correct.

Q Okay.

BY MR. PARLER:

Q I gather that what you have been talking about is around November 27, 1978, SECY, S-E-C-Y, paper 78-616, a paper from Harold Denton to the Commissioners entitled Reporting the Progress of Resolution of Unresolved Safety Issues in the NRC Annual Report, and there is a companion paper which is in the book that I just showed Dr. Hanauer, a paper 78-616A, which is responsive to the concern of the Commission about certain items that the Commission believes should be included on the unresolved list, one of which was Task A-17, Systems Interactions of Nuclear Power Plants.

But the reason I had this book out, Dr. Hanauer, was to ask you if the draft report of the probabilistic analysis staff, which is in this Staff paper, SECY-78-616, is it still a draft report, or has that group submitted its final report?

I can show you what I'm talking about if my question isn't clear.

mpb68

#8

MR. PARLER: Let's go off the record while I'm looking for this.

(Discussion off the record.)

MR. PARLER: On the record.

BY MR. PARLER:

Q Dr. Hanauer, to the best of your knowledge and recollection, has the probabilistic analysis staff draft report or draft summary report on a risk base categorization of NRC technical and generic issues, has there ever been a final report to your knowledge put out by that staff on the subject?

A I don't know.

Q Okay.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. PARLER:

Q Before the luncheon recess there was some reference to a Commission decision on a Union of Concerned Scientists' petition about the environmental qualification of electrical connectors.

MR. PARLER: And I gather that you're going to get, Mr. Scinto, a copy of the Commission's decision for Dr. Hanauer to look at. Would you proceed with that, please, sir.

mpb69

MR. SCINTO: Yes.

BY MR. SCINTO:

Q Dr. Hanauer, I believe during the break you have gotten a copy of the Commission decision I was referring to. It's an April, 1978, decision in connection with the petition of the Union of Concerned Scientists.

A Yes, sir. It's to be found in Nuclear Regulatory Commission Issuances, Volume 7, number 4, and it starts on page 400.

Q Among the issues touched on by the Commission in that decision is a brief -- I believe a brief discussion of the single failure criteria as it was raised in the context of that issue.

A It's done twice, and the two discussions are almost identical. The better one is in the middle of page 427.

Q The question I would ask, Dr. Hanauer, is:

You had in connection with your decision -- Mr. Parler had identified -- I need the exhibit on single failures.

MR. PARLER: Okay. I'll get it for you.

THE WITNESS: The one on single failures or the one on -- the Gilinsky memo.

MR. PARLER: 1135.

THE WITNESS: It's that one.

BY MR. SCINTO:

Q In connection with your discussion with Mr. Parler

mpb70

earlier today in connection with Exhibit 1135, I believe you noted that you had -- that this memorandum you wrote to Commissioner Gilinsky had pointed out some problems associated with the application of the single failure criteria.

My question to you is:

How would you characterize the Commission's discussion of the single failure criteria in the UCS petition as it bears upon the problems you discussed with Commissioner Gilinsky? Is it beneficial, is it not beneficial? How would you characterize the -- whatever guidance there is in that Commission decision with respect to the single failure criteria?

A It doesn't treat this problem at all.

Q Thank you.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

BY MR. PARLER:

Q Before we go into other areas, Dr. Hanauer, there are a couple of other questions in the safety area that I would like to ask you.

I understand that in the regulatory area, particularly in technical specifications for nuclear power plants, that there is such a thing as safety limits, and such a thing as safety margins.

Am I correct thus far?

mpb71

A Yes. You're outside my expertise.

Q All right.

A I don't deal with technical specifications much.

Q All right.

The question that I was going to ask you -- but I will honor the statement that you just made, but let me go ahead and ask the question -- is:

How does the NRC establish the things that have to be covered as safety limits to provide reasonable assurance that the public health and safety is protected against undue risk?

If that question is outside the area that you're involved in, please so indicate and we will move on to something else.

A I'll give you a short answer.

There's a group that works on this subject pretty much constantly reviewing tech specs and issuing improved editions of standard tech specs which have been developed for the classes of plants.

The question, the more interesting question is: how is it decided which things should have tech specs based on them at all? There is no simple answer. This is based on operating experience, review experience, accident analysis, particularly in Chapter 15 of the Safety Analysis Report which shows not only what the assumed values of the parameters are,

mpb72

but what the sensitivities are in the SARs and in technical reports which we have required to be submitted.

This tells us what are the things that are important to the safety analysis and important to the safety of the plant, and those are the things we write tech specs about.

Q Fine.

Dr. Hanauer, the reason that simple question was asked by this layman is because it would appear in numerous places that decisions in the regulatory area are made on the basis of engineering judgment, and I was wondering how the process worked so that the engineering judgment could deal with refinements such as things such as safety limits, which would be what I would understand to be the hard core that is required for safety purposes, and then safety margins.

But I think you have answered my questions. I was just explaining to you why I asked it.

MR. PARLER: Mr. Lanning, would you ask the quality assurance questions, please, about the Browns Ferry recommendations?

BY MR. LANNING:

Q As part of your investigation into the Browns Ferry incident, were there recommendations concerning quality assurance programs?

A Yes, there were. They are to be found in

mpb73

NUREG-0050. They are summarized in Section 1.6.4, starting on page 6, and they are discussed in additional detail in Section 5.2 on page 49 and in Section 6.3.2 on page 57.

Q Are there any of those recommendations that in your mind are more important, that require Commission attention?

A More important than what?

Q Than the others?

A Well, I have to remind myself of them. The report is now four years old.

(The witness reviewing document.)

Let me just characterize them and talk about them briefly.

The first recommendation related to the demonstrated inadequacies in the Browns Ferry QA program. The study group did not consider or evaluate the new program which was reviewed in the usual way, and I haven't reviewed it and don't have an opinion about it.

The quality assurance requirements were being revised and the application of the quality assurance requirements to the plants was in a state of flux at that time, and in fact the Browns Ferry quality assurance program had never been reviewed.

The special review group formed to evaluate the Browns Ferry fire, of which NUREG-0050 is the report, stated QA programs of all nuclear power plants' licensees should be

mpb74

reviewed. QA programs in some operating plants that are known not to conform to current standards should be upgraded promptly.

As far as I know, this review has been completed. I don't know how prompt it was. The NRC review of licensee QA programs should be correspondingly upgraded in particular to include explicitly fire protection. This has been done. And provisions to maintain important functions in spite of a fire. This has been done.

So the explicit recommendations have been accomplished.

Q Are you aware that there is not a criterion in Appendix B requiring or addressing maintenance, preventive maintenance?

A No, I haven't read Appendix B in years.

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: Back on the record.

Let me try to ask this question.

BY MR. PARLER:

Q Dr. Hanauer, some have representative their belief that the adjudicatory process in the licensing of nuclear power reactors has an inhibiting effect on full discussion of the safety issues by the Staff in its Safety Evaluation Reports.

bu8

I guess the first thing I should ask you is:

mpb75

Have you had any experience in adjudicatory proceedings before Atomic Safety and Licensing Boards?

A Never in a licensing case; only in a rulemaking hearing.

Q With that understanding, that your experience has been limited to rulemaking hearings, do you have any comment on the view that I have just tried to express that some people have, that is that the adjudicatory process could have a negative effect on the quality of the Safety Evaluation Reports?

A I've never experienced it, and I worked for many months in the generation of Safety Evaluation Reports as assistant director for plant systems.

Q Okay.

Dr. Hanauer, one of the issues that the Special Inquiry Group is looking at is the rush to commercial operation issue by Metropolitan Edison.

In your regulatory experience have you been involved in issues that relate to commercial operation or placing a plant in commercial operation?

A Not at all.

Q Have you ever been involved in the structure of the testing programs and the power ascension program -- that's a-s-c-e-n-s-i-o-n was what I was trying to say --

A Yes. I've looked at some of them.

mpb76

Q Do you happen to recall whether there is anything that would be a useful benchmark in that area that is to be used for comparing schedules for tests to see whether one is a reasonably thorough approach on a realistic schedule or are these things, generally speaking -- these things being the testing programs, et cetera -- largely dependent upon particular plants and individual situations?

A I don't have enough experience to comment.

Q All right.

Dr. Hanauer, at this point I have finished the questions I have to ask you. I will now turn this over to Mr. Scinto.

On behalf of myself and my colleagues I would thank you very much, sir, for your cooperation and help.

Mr. Scinto?

MR. SCINTO: Right.

Are you packing up?

MR. PARLER: Off the record.

(Discussion off the record.)

MR. PARLER: On the record.

BY MR. SCINTO:

Q Dr. Hanauer, my questions will be aimed in a different direction. I am going to get into some detail into your personal participation in the Commission's response to the Three Mile Island accident.

mpb77

When were you personally informed that there was an incident or an accident involving the Three Mile Island facility?

A I don't guess I remember. I'm going to consult my log --

Q Please do.

A -- of Three Mile Island, which has already been furnished to you. It's entitled "Three Mile Island Accident, S. H. Hanauer, Log Book Number 1".

I knew about it on the 28th, but I don't remember how I found out. And I did not participate actively in it until a couple of days thereafter. On March 30th I was at an ACRS Subcommittee meeting in Phoenix. Before I left on the 29th I called the incident center and talked to Mr. Case to get an update as of that time because I knew the ACRS Subcommittee would want to hear it.

I went to Phoenix. I did my thing for the morning of the 30th. At noon I received a telephone call from Mr. Tedesco instructing me to return, which I did.

After some vicissitudes, I checked into the incident center at about 2 a.m. on the 31st of March.

Q Fine.

There are two things I wanted to make clear:

In the course of the deposition you may very well be referring to notes or documents. I'd like to make it clear

mpb78

at times when you're relying on the document for the information and when the document is being used for your personal recollection.

Most of my questions are going to be directed to your personal recollection. And if you don't recall them, you know, that's perfectly okay too. A lot of material that's in documents we can find in the documents, and I don't need to ask you to repeat material that's in a document. So whatever it is, make it as clear as you can, okay?

Okay.

So you've indicated that you had a brief telephone conversation on the 30th with Mr. Case.

A 29th.

Q On the 29th.

That would be Thursday?

A Yes. That was not my first inkling of the accident, but I was getting updated.

Q Your first inkling I'm now willing to go past.

It was an updating on the Thursday, the 29th, before you left for Phoenix?

A Yes.

Q Was that early in the day or late in the day?

A Noontime.

Q Fine.

Do you recall the gist of what Mr. Case told you

mpb79

about the condition of the reactor, particularly the condition of the core?

A Yes, and it's also on the incident center tape. I don't recall what terms we used; we discussed the sequence of events that had happened on Wednesday, the activities of the operating staff.

My recollection is -- and I'm quite clear about this -- that it was clear to me that the core was substantially damaged at that time.

Q Was it your impression from that phone call that conditions then, on Thursday at noon, were generally stable?

A Yes, that was the impression I got. But neither Mr. Case nor I, in talking it over, felt that we had really reached a stable situation.

Q By that last comment, you mean the long term stable situation?

A No. The core was felt by the operators to be in a stable situation. The primary coolant pump was running. The temperatures were coming down. But we were uneasy about it. We didn't feel there was any immediate -- we felt that it was all right for me to go to Phoenix, for example.

Q I'm trying to draw your recollection back to that conversation at that time before you left for Phoenix.

A Yes.

Q Did you have in mind a picture of a core in which

mpb80

there had been a significant amount of metal-water reaction? What was in your mind?

A What was in my mind was a fairly unspecific picture of a damaged core. I saw the gap activity pretty much out. I don't remember whether I felt metal-water or not.

Q Now you indicated the reason you wanted to get filled in on the current status on Thursday is you felt that the ACRS Subcommittee that you were going to attend a meeting of would want to know.

A Yes.

Q Did you inform the ACRS Subcommittee?

A Yes, I did.

Q And generally conveyed the picture you conveyed now?

A Yes. I discussed the sequence as we then understood it, and the situation in the core as we then understood it.

Q Anybody ask about significant generation of metal-water reaction, a significant amount of metal-water reaction?

A I don't recall it, but it wasn't an important thing that I would be likely to recall.

Q Fine. Okay.

I think you just testified you were called on Friday, the 30th --

A Yes.

mpb81

Q -- and asked to return from Phoenix.

A Yes.

Q Generally what was the gist of the information you received on the phone call asking you to return?

A I got very little information, except that everybody was getting tired out. It looked as though it was going to be a fairly long drawn-out thing and I was needed.

Q Okay.

A I remember Mr. Tedesco saying that we seem to have releases at least comparable to TID releases in the containment and maybe higher.

Q Okay.

Now approximately what time was this phone call?

A About noon on Friday.

Q Okay.

In that conversation on Friday, do you recall being informed that there was a very high activity primary coolant sample taken?

A No, I don't recall that. The idea that everything was very radioactive was clear, and as I just testified, we -- Mr. Tedesco told me that the activity in containment was very high.

The sample I don't recall hearing about.

Q You I believe just testified that you arrived back in Bethesda at around 2 a.m.

mpb82

A I arrived at the incident center almost exactly at 2 a.m.

Q That was going to be my question, was where.

A I went directly from the airport.

Q To the incident response center?

A Yes.

Q Okay.

Now when you got to the incident response center who was there?

A Oh, I don't have an organized recollection. People came and went.

Q Do you recall who the senior Staff people were?

A I reported in the next few days to one of three people who rotated. They were Don Davis, Darrell Eisenhut --

Q I think in your Presidential Commission deposition you mentioned Brian Grimes.

A Yes, Brian Grimes.

Q Okay.

I recognize that -- I'm trying to push your memory --

A Mr. Case came and went, Mr. Gossick came and went, Commissioners came and went. I can't tell you was there at the moment.

Q Fine. I am pushing your memory, and if you can't recall --

mpb83

A No, I really can't.

Q Okay. Fine.

Now when you arrived at 2 a.m., did you then undertake any duties?

A Yes.

Q Okay.

What were the duties, briefly described, you undertook commencing about 2 a.m. on that Saturday morning?

A I'm now refreshing my memory from my notes taken at that time. These are the notes which I made at that time.

The first thing I looked into was the radiation of the reactor coolant pumps. We had gotten a note from Babcock and Wilcox that the main circulating pumps might have a problem with the radiation resistence of the condensers. I copied out of various references and organized the information on the main circulating pumps and their components and the radiation resistence.

I talked to Mr. Taylor of Babcock and Wilcox and concluded that there was no immediate problem in spite of the earlier message from Babcock and Wilcox, furthermore that if we didn't shut the pumps down they would continue to run even if the condensers went out, unless the condensers short-circuited and blew the braker.

I then worked for a while with a group of people, whose names I didn't write down and no longer recall, on

mpb84

#9

questions related to how to burp the system of the hydrogen bubble then thought to be in the system. And I wrote down some things which were being considered and listed a long list of contingencies that had been considered.

It became clear fairly quickly that a whole lot of good people had been working on that problem for quite a long time and that I was not making any contribution to it.

Q Before you took on the work in connection with the reactor coolant pumps, which you indicated was a first activity, were you briefed on the condition of the system and the core at that time before you undertook the work?

A No, except in the most cursory way.

Q Okay, fine.

If you can recall from that gathering of information, did you then have a mental picture of the condition of the core before you started to work on reactor coolant pumps?

A Not anything significant, except that I do recall looking at maps of thermocouples and looking at some curve somebody had plotted on some trends, and the temperatures were quite high but they were coming down.

Q About how long -- about when did you complete your work and reach your conclusion that the pumps -- that there was no immediate problem with respect to the pumps?

A I don't have that time noted. It didn't take very long.

mpb85

Q Early morning Saturday?

A Early Saturday morning, because I worked on some other things too.

Q Okay.

Before you started working on the matter of burping the system of the hydrogen, I assume that you had been told that there was a big bubble of hydrogen?

A Yes.

Q Generally what was the gist of what you were told about the hydrogen in the system?

A Well, I have no notes on this. I'm working from recollection.

I was told that measurements of pressure and volume showed an elasticity of the system which indicated that there was a bubble in the system and that this was thought to be in one or more of the following locations: the reactor vessel head, the top of the candy canes, and perhaps in the reactor coolant pumps, although that's not as clear in my recollection, and, of course, in the pressurizer, which was known.

And I discussed with a group that was working continuously on the problem how these were being measured. And at various times it was described as a gas bubble or a steam bubble.

There was some indistinctness about what was in the

mpb86

bubble, but the word "hydrogen" was pretty generally used.

Q Can you recall the leaders, the group leaders or some of the people working on this project who did perform this?

A I vaguely recollect that Warren Minners was in the middle of this, and others who I don't distinguish any more.

Q Were you specifically informed or told about the recommendations earlier on that day, Friday, by members of the Commission Staff and by the Commission concerning evacuation of the general area around Harrisburg? Were you informed of that about that time when you first started to work?

A I don't know. I've seen too many versions of it since to know when I was informed.

Q Thank you. That's important to identify and that's exactly what we do in these cases. Okay.

I'd like to proceed a little bit further on Saturday. You said you started to work about 2 a.m.

How long did you work on Saturday? When did you leave, if at all?

A My recollection is that I worked until about noon. I don't have a note.

Q And then what? Did you leave?

A Then I went home and slept.

Q Okay.

Did you return on Saturday?

mpb87

A Yes, I came back Saturday night at 10:55.

Q Okay.

I now want to deal with the portion of the time in the morning and not the evening work. I'll come to the evening in a moment.

We talked about, in that morning period of time, from the time you arrived until the time you left you worked on the question of the reactor coolant pumps, about burping the system. What other projects?

A I worked on lead bricks.

Q What about lead bricks?

A I got a request from the site to please find them a lot of lead bricks to shield the recombiners. I called Naval reactors and Mr. Broadsky looked into it and called me back and told me, correctly, that he had found what he described as an "acre of lead bricks" 20 miles from the site. And he had trucks loading up these lead bricks and he wanted to know where they wanted them arranged, where the lead bricks should be delivered.

But in the meantime there was some bureaucrat in GSA who was in charge of these lead bricks, and he wanted to talk to us. So I called Mr. Mitchell in the GSA. They were part of the national strategic stockpile of lead bricks, and he said he wouldn't release them except on the word of the -- quote -- "Federal official in charge", who he identified

mpb88

as the regional director of the Federal Disaster Assistance Administration.

In the meanwhile, Broadsky's trucks and drivers had in fact loaded up some 60 tons of these bricks and transported them to the site. But I was careful not to tell him this. So we got the bureaucratic affair straightened out after some dozen or so telephone calls.

Q Did you pursue the rest of it through the way of --

A I pursued the rest of it and finally at one point gave up and got whoever was in charge of the incident center at that time to pursuade whoever was on the other end of the White House line to give Mr. Mitchell a call, after which the problem went away.

It furnished some amusement in the long night.

THE WITNESS: Off the record.

(Discussion off the record.)

MR. SCINTO: On the record.

THE WITNESS: Continuing the answer to the question, I must have done some other things that morning, but I made no notes and have no recollection.

MR. SCINTO: Okay.

BY MR. SCINTO:

Q Do you recall at any time in the morning period being informed of or otherwise being aware that there was a concern about a potential generation of oxygen in the primary

mpb89

system?

A My recollection is that I didn't know much about oxygen until that evening, but this is very indistinct and I could have found out about it that morning.

Q You don't have a present recollection of that?

A No, I don't. I was only at the edge of the oxygen question.

Q So that morning you weren't working on oxygen?

A No.

Q Right. Fine.

When did you personally become aware that the hydrogen recombiners were not installed on TMI Unit 1?

A On TMI Unit 1?

Q Oh, sorry, sorry; TMI Unit 2.

A I knew about that quite early, that they were going to couple them up in an hour, and then they were going to couple them up later, and then they were going to couple them up... And for several days all we heard about was when in the near future we were going to get those combiners coupled up and turned on.

Q In view of your personal rather long background in the regulatory process, in which there was some association with recommendations that hydrogen, post-LOCA hydrogen control in containment be a problem to be focused on -- I think, for example, this morning in connection with Mr. Parler's portion

mpb90

of this deposition you referred to a letter which you had written as chairman of the ACRS in connection with Three Mile Island suggesting that there be some hydrogen -- some facility for hydrogen, post-LOCA hydrogen control.

Did that surprise you to find, when you started to work on Three Mile Island 2, the response at the incident that the hydrogen recombiners had not been installed in this unit?

A No. The theory of the hydrogen recombiners was that they were too slow to work on the early puff of hydrogen calculated to occur in the loss of coolant accident, which was, of course, below the flammability limit. And in those plants where it wasn't, they had to be inerted.

The theory of the hydrogen recombiners was that there were a lot of days available in which to hook them up and what they needed to be was onsite or immediately available for coupling up in a time short, compared to a few days. So I wasn't the least bit surprised.

Furthermore by that time we had a containment sample that had a modest amount of hydrogen in it, and the calculations were that we had plenty of time.

Q Okay.

Now I'd like to go to Saturday evening after you returned.

A Yes.

mpb91

Q Now did you undertake any activity Saturday evening?

A Saturday night, the whole night from when I came in until the next day about two o'clock I was in charge of a task force to develop criteria for evacuation. There's a lot about this in my deposition to the Kennedy Commission.

Q Who assigned you this responsibility?

A Dr. Mattson, M-a-t-t-s-o-n.

Q Basically what was the gist of what he told you he wanted you to do?

A I'm working both from my recollection and from my notes.

Q Okay.

A He told me that what was desired was the criteria for evacuation in the form of a table in which one would have decision criteria, namely if certain conditions obtained or certain events occurred who would decide how much warning time we would have and what should be done.

Q Now were you informed at that time or at any time that those criteria might be a matter to be used by one or more Commissioners?

A Oh, yes. Commissioner Gilinsky's name was used.

Q Okay.

Now how did you accomplish this task? Did you form a group?

mpb92

A Yes, we formed a group. We looked briefly at the kinds of people we needed, and I asked Dr. Buhl, B-u-h-l, to come in and work with me on it, which he did. We then assembled a group which at various times during the night had between four and eight people.

We divided -- I have here one list, nine people plus Dr. Buhl and me and others who were involved during the night, although not everybody at once. We divided the job into -- I don't know how much of this you want -- we divided the job into --

Q As much as you recall.

A -- engineering problems and dose problems. That is to say, the engineers considered what are the possibilities of what would happen in the plant and what kind of releases would this give, and the dose people translated these releases into doses on which we would judge what to recommend on -- in the way of evacuation.

Dr. Mattson also wanted us to consider developing a list of things in which we might consider recommending evacuation before some particularly hazardous operation. His example was if we decide we have to turn on the RHR and circulate the primary fluid outside containment, we might consider -- we should consider whether we should evacuate people before we do that as a precaution.

We then, in the course of the evening, we also

mpb93

decided to -- thought about developing -- we didn't do all these things -- about developing a list of things not to do unless you absolutely have to. If the weather is bad -- weather bad in this case meaning dispersion is poor -- the things which if you decide to do them you take precautions first, things people oughtt to be doing right now. For example, firing up the auxiliary boiler for aux feedwater, deciding what to do with the spare recombiner.

I guess when I wrote that down I didn't realize that the recombiner still wasn't running. This was an on-again, off-again proposition for several days.

And finally, the bottom line: What should they do if they thing the core has melted or is about to melt, and how would you find out.

We then divided our people up to study these various alternatives. At one point some people tried to start some calculations on fault trees and event trees, but as might be predicted, that never got anywhere in the time we had available to us.

We considered the weather possibilities, what the weather was then, what the forecast was, what the possibilities were. We considered some options for modes of evacuation, should it be everybody within a certain distance or should we try and specify some particular direction, everybody who lives northeast of the plant should move.

Our decisions in this were later changed by the Commission, who had been talking to the people in Pennsylvania about what was practicable. I then have various results of fragmentary calculations about 'suppose this happened, what would the release be, what would the doses be'.

We then produced a draft document which has been furnished. My notes get more and more fragmentary. We then produced a draft document which has been furnished, which has a bunch of attachments to it.

Q Dr. Hanauer, I'm about to show you a document which seems to be a compilation of a number of documents. It has a total -- I have counted a total of 23 pages, even though they're not numbered. They have been previously identified to a member of the study group -- the Special Inquiry Group, at least the first seven pages of which were provided by one of the Commissioners to the people of the State of Pennsylvania on Sunday, April 1st, at least the first seven pages.

I'm wondering whether you can help me identify various other portions of this thing.

A There were two papers, there was an earlier draft which was provided to Commissioner Gilinsky, and slightly later Commissioner Ahearne, and Commissioner Kennedy came in a little later. Chairman Hendrie, as I recall, was already at the site.

Who did I leave out?

mpb95

Q Bradford?

A Commissioner Bradford came in somewhat after Commissioner Gilinsky, with the others.

This document you handed me is in fact a hodge-podge of these two or three documents, of which I may or may not have adequate copies.

MR. SCINTO: I'm going to take the opportunity right now to ask the Reporter to mark this document with the next number in the sequence.

(Whereupon, the document referred to was marked as Exhibit number 1148 for identification.)

THE WITNESS: What you have is in fact the second document which was produced, the first one being an earlier draft which didn't go anywhere. But you have it combined with a -- all right.

The document you handed me -- I don't know if you want to mark it or not.

MR. SCINTO: It's been marked. I marked it in the interim while you were looking.

THE WITNESS: What's its number?

MR. SCINTO: 1148.

THE WITNESS: 1148.

This document was, as corrected from an initial

mpb96

document after discussion with the Commissioners and Mr. Grimes and Mr. Murphy, who made major contributions toward the last, in making some sense out of a not very coherent first draft, and indeed these seven pages went to Pennsylvania.

The rest of this document -- in fact, the first three pages of it are marks by me on the three pages of what went to Pennsylvania. Commissioner Gilinsky asked me -- left a copy of this for me and asked for my comments, which I gave him.

So the eighth, nineth and tenth pages are my recommended pages in what went to Pennsylvania, or at least in what he left for me. I don't know if they went to Pennsylvania or not.

The tenth through 21st pages are some of the earlier work which was used as a backup to explain the work that's in the front. And so what you have is rather a composite of three documents on the same subject, and there's some considerable overlap.

MR. SCINTO: Fine. Thank you for the help. That does help a lot in sorting this out.

THE WITNESS: In working out the last answer, I consulted some other of my notes, which is a notebook containing a large number of documents that came to hand during the accident and which has also been furnished.

MR. SCINTO: We've marked this document. I will

mpb97

ask a couple of questions about it. But I'd like to make clear I'm not really asking you for what the document says. It says whatever it says.

THE WITNESS: Yes, it does.

MR. SCINTO: There are some things in there that I want to ask you about in connection with what you knew or what information you received and your work on it. I use the document as a reference for that purpose.

But if they are not things that you are familiar with, just say you don't recall that or something, it's something you're not familiar with. Okay.

BY MR. SCINTO:

Q Among the things in this document, toward the end of the document is a page that I have marked on the lower left hand side with the letter T.

A I have it.

Q It indicates there was some thought for the potential for a hydrogen explosion in the reactor pressure vessel. That's what it indicates.

A By this time that was a hot topic.

Q That was my question.

A This was a hot topic. During the course of this night there were heated and lengthy discussions among a lot of people which I was on the fringes of, in general, in pursuing my appointed task about the hydrogen explosion potential in the

mpb98

reactor pressure vessel.

I remember at one point during this period -- I can't tell you exactly when -- I stopped what I was doing and looked up some hydrogen solubilities. But I can't tell you when that was.

Q That was hydrogen solubilities?

A Yes. We were still trying to get the hydrogen out of the bubble by using differential solubility techniques.

I remember discussions of the possible trigger mechanisms for a detonation. I remember discussions of the pressures that might result if a hydrogen bubble of a certain size exploded in the reactor vessel or if a hydrogen bubble of a certain size burned without explosion in the reactor vessel.

This was going on essentially the entire night while I was working on evacuation. I have, for example, a note toward the end of my notes on that night:

"Hydrogen mixture in explosive range."

That is one of the conditions which would require consideration of evacuation.

Q That was a note that indicates one of the things you wanted to do, rather than a note of it was in that condition?

A No, no, that's not what it means.

Q Okay.

Do you have any recollection -- strike that. I

mpb99

would like to phrase that differently.

From what you've described, then, it does not appear that by that time of the evening on Saturday there had been a significant diminution in concern?

A I think it depended on whom you talked to.

Q Fine.

A And I can't put names to this any more, but there was a spectrum of opinion. Some people were very concerned based on the information they had. People were on the phone all over the offices all over that building with all kinds of experts of various aspects of the problem.

I cannot give a connected account of what people thought at various times during the evening.

Q But you do recall discussions relating to possible ignition sources?

A Yes.

Q It was not -- from what you can recall of those discussions, would you have gotten -- was it your general impression that there was in general in the people working on the problem in that evening little concern?

A Oh, no. There was a spectrum of concern, but a lot of people were very concerned.

Q No, there was little concern about the potential for sources of ignition?

A No, that's not true. There was at least one person

mpb100

on the phone a lot -- you understand, I was in and out --

Q Right.

A -- on the phone a lot with people about what could be the ignition sources. And I remember he talked to somebody who understands such things, and they were talking about molecules of liquid jumping into the gas from thermal agitation and forming hot little centers which could be sources of ignition.

Q I know you said you couldn't indicate -- you couldn't identify names in your mind, but perhaps this might refresh your recollection.

We've had some testimony in some of our depositions identifying that kind of a concern associated with Dr. Budnitz.

A Yes, that's where I heard it. But the discussions were more general than that. He was just, if I understood it, the one who had gotten that particular message from somebody who was supposed to know.

Q Okay.

If you recall, do you recall any discussions concerning the potential for hydrogen recombination resulting in a situation where there was no need at all to be concerned?

A Not that night, I don't.

Q Okay, fine.

And I again am pressing your recollection for that.

A That's right.

Q Right.

mpb101

A Our paper would have been quite different if that had been a significant thought.

Q Fine.

This document, again directing your attention to page T, in the lower left-hand corner indicates that:

"A rough analysis indicates that the pressure vessel would not rupture with detonation of the hydrogen bubble."

I believe that is a correct characterization.

Do you recall where this information came from?

A No, I don't. And I have seen information since that's contrary to that, that the pressure which probably wouldn't rupture the vessel comes from burning rather than detonation. That was the best information at the time, and I don't know where it came from.

Q All right, okay.

Another sentence is:

"The postulation of the core response is difficult."

Do you recall that evening a concern that the core might be so fragile that it would be detrimental, perhaps, to start a second reactor coolant pump?

A Yes, I do recall that.

Q With that --

A I'm not sure it was that evening.

mpb102

Q Okay, all right. Fine.

No matter when it was, if that was the fragility of the core that there was a concern about, if people were concerned it might be that fragile -- I guess I'm having trouble identifying how they thought the core would respond to the kinds of events that would be associated with either burning or explosion.

A Well, burnir~ does not necessarily disrupt even a fragile core. If the core were that fragile then detonation would break it up. So that we -- at least we weren't thinking about it when we wrote that sentence. That's all I can say at this time.

Q Fine.

I'm trying to get your recollection of that time.

I'd like to direct your attention to a page that I have marked on the lower left corner with an H. It has on it on the top a note which appears to be a note from you to Commissioner Gilinsky.

I'd like to refer on that page to an event in the event series, an event characterized as "depressurization". In that event in postulating the various responses that might occur with respect to that event, was this now a picture of depressurizing that core with a very large hydrogen bubble in the head, the reactor vessel head?

A No. They thought there was -- that suppose we

mpb103

decide or are forced to depressurize the system to go on RHR, but clearly we were not thinking about the depressurization would uncover the core, because the expected plant responses are not consistent with that.

Q On this table, a similar table, a table very similar that was used in the first seven pages, on this table there is a column described as "Warning Time".

Do you recall what the people that prepared the table, if you participated in the preparation of the table, had in mind by the concept of "Warning Time"?

A This is the time between when you knew you had trouble and when doses would start to get to people.

Q Okay, fine.

A Now that's from a lot of recollection, and it may be -- I don't know whether there's an allowance for the transport of the material outside or whether this is the amount of time until you ought to start evacuating; I don't think so. I think I described it correctly at first.

Q Okay.

One of the things that I don't mind repeatedly making clear is that I am intending to push your memory.

A Yes.

Q I would like to turn to the next page in this connection, that same column. There is a distinction in warning time between a sequence of events leading to core melt,

mpb104

one in which containment integrity is maintained and one in which containment integrity is breached. There is a different warning time in those events where containment intergity is likely to be maintained of four hours, and a warning time in those events in which containment integrity is expected to be breached of 24 hours.

I'm trying to understand that distinction. Does that suggest that there is a 20 hour warning time between the time you can distinguish between an event which is going to maintain containment integrity and one which is going to breach it?

A No. What was meant was this:

Remember, the initiating event is the sequence leading to core melt. The sequence tells us that some -- no, I'm sorry, I'll start over again.

The Reactor Safety Study tells us that all core melts breach containment, some very quickly and some very slowly, and in a rather benign way. By this time the reactor had been shut down for four days, and so the probability of containment breaching was much lower than in the Safety Study.

The point here was that if the containment was going to breach it would take it about 24 hours, and so the situation would, even if containment was going to breach, degenerate from the top line to the bottom line, and that there would be of the order of 24 hours' warning if the

mpb105

containment was going to breach, so that you would have four hours' warning for the smaller evacuation and 24 hours' warning if you had to go to the larger evacuation, at least so I reconstruct it.

bu9

Q Now --

A Now let me note something on this same page.

Q Sure.

A The next role of discussion relates to hydrogen explosion inside the reactor vessel, and my notes of April 2nd show a different perception of what the risk was for hydrogen explosions or flames inside the reactor vessel, and show a much lower perception of risk.

Q When you refer to your notes of April 2nd, what are you referring to?

A The handwritten notes which were part of my transmittal to Commissioner Gilinsky, on the page marked I.

Q Right.

The reason I ask is I had misread that as April 1st. Thank you for making that correction. All right.

Now the mechanism for breach of containment postulated in the sequence we were just talking about, what was that mechanism? Was that a detonation of hydrogen in containment?

A Oh, no, it was a melt-through. By that time the hydrogen in containment, the concentration was quite low, not even in the flammable range, presumably because of the oxidation mpbl06

incident that took place the first day.

Q Okay.

I'd like to direct your attention to a portion of this document, to the page that I have marked Q. There appears to be two events described in a time sequence, one in which the containment survives and one in which the containment fails. There are different assumptions for these events, and I think that they conclude with the significance of the sprays and coolers, and some reference to hydrogen being combined or otherwise removed from containment.

Actually I'd like to direct your attention to the line that reads:

"Containment survives." It's underlined.

"(Failure assumed 2300 psi)"

Now do you recall this?

A Not very well, but I'm rebuilding it in my mind from these notes.

Q Okay, fine.

And if I'm asking questions that you don't have a recollection of at that time, you know, stop. There's no use....

We have, as you've pointed out before, we have a significant quantity of post-accident recollections or post-accident --

A Yes, it's important to try to avoid contamination.

Q Yes, that's what we'd like to try to do. We have

mpb107

a lot of those. We have a lot of documents, we have a lot of depositions, we have depositions from people taken later.

What I'm doing at this time is pushing your memory for those evenings.

A Yes.

Q Okay.

With the concept that containment failure was assumed to occur at 130 psi, was that concept directed principally at the massive structure of containment, or was that concept equally applicable to other parts of the containment boundary penetrations, particularly I'm thinking of the large vent openings, the purge openings and vent openings.

A I don't know.

Q Okay.

A It's a number which was derived by the Safety Study people who were working with me, Joe Murphy, Roger Blond, and Tony Buhl. I don't know where they got it. I may have known then, but probably not. And I don't know whether they included that or not. Joe Murphy would be the person to ask if you really want to know.

Q Right.

MR. SCINTO: Off the record, please.

(Discussion off the record.)

(Whereupon, at 4:50 p.m., the deposition in the above-entitled matter was adjourned, to reconvene at 9:00 a.m., the following day.)

Ex #.
Exhibit
1031

Biographical Sketch

STEPHEN H. HANAUER

1979

1979-present	U.S. Nuclear Regulatory Commission Director, Unresolved Safety Issues Program Supervision of 20 task groups effecting the generic resolution of the most important and urgent reactor safety issues.
1978-79	U.S. Nuclear Regulatory Commission Assistant Director for Plant Systems Division of Systems Safety Directing three branches (Instrumentation and Control Systems Branch, Power Systems Branch, Auxiliary Systems Branch) in safety reviews of CP and OL license applications.
1970-78	U.S. Nuclear Regulatory Commission Technical Advisor to the Executive Director for Operations Principal staff advisor to agency executive officer, primarily on technical safety issues.
1965-70	Professor of Nuclear Engineering, The University of Tennessee Undergraduate and graduate instruction; supervision of Master's theses and doctoral dissertations; research in theoretical and experimental reactor technology.
1950-65	Physicist and Development Engineer, Physics Division and Instrumentation and Controls Division, Oak Ridge National Lab Development of reactor instrument systems and components; design, installation, and operation of instrumentation and control systems in a dozen Oak Ridge reactors; research in reactor noise analysis; reactor safety considerations.
1965-70	U.S. Atomic Energy Commission, Advisory Committee on Reactor Safeguards. Vice Chairman - 1968; Chairman - 1969 Statutory technical committee reviewing license applications and other safety matters.
1962-78	International Electrotechnical Commission, Chairman, Subcommittee 45A, Reactor Instrumentation.
1962-present	Member, American National Standards Institute, Committee N42, Nuclear Instrumentation.

Born March 6, 1927
Bachelor's and Master's Degrees in Electrical Engineering, Purdue University
Ph.D. in Physics, University of Tennessee

Exhibit 1030

September 6, 1979

In Reply Refer to:
NTFTM 790906-02

Dr. Stephen H. Hanauer, Assistant Director
for Plant Systems
Division of Systems Safety
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Dr. Hanauer:

I am writing to confirm that your deposition under oath in connection with the accident at Three Mile Island is scheduled for September 25, 1979 at 9:00 a.m., in Room P-822, Phillips Building. This will also confirm my request for you to have your resume and any documents in your possession or control regarding TMI-2, the accident or precursor events which you have reason to believe may not be in official NRC files, including any diary or personal working file.

The deposition will be conducted by members of the NRC's Special Inquiry Group on Three Mile Island. This Group is being directed independently of the NRC by the law firm of Rogovin, Stern and Huge. It includes both NRC personnel who have been detailed to the Special Inquiry Staff, and outside staff and attorneys. Through a delegation of authority from the NRC under Section 161(c) of the Atomic Energy Act of 1954, as amended, the Special Inquiry Group has a broad mandate to inquire into the causes of the accident at Three Mile Island, to identify major problem areas and to make recommendations for change. At the conclusion of its investigation, the Group will issue a detailed public report setting forth its findings and recommendations.

Unless you have been served with a subpoena, your participation in the deposition is voluntary and there will be no effect on you if you decline to answer some or all of the questions asked you. However, the Special Inquiry has been given the power to subpoena witnesses to appear and testify under oath, or to appear and produce documents, or both, at any designated place. Any person deposed may have an attorney present or any other person he wishes accompany him at the deposition as his representative. The Office of the General Counsel of NRC has advised us that it is willing to send an NRC attorney to all depositions of NRC employees who will represent you as an individual rather than represent NRC. Since the NRC attorney may attend only at your affirmative request, you should notify Richard Mallory (634-3224) in the Office of the General Counsel as soon as practicable if you wish to have an NRC attorney present.

You should realize that while we will try to respect any requests for confidentiality in connection with the publication of our report, we can make no guarantees. Names of witnesses and the information they provide may eventually become public, inasmuch as the entire record of the Special Inquiry Group's investigation will be made available to the NRC for whatever uses it may deem

OFFICE ▶						
SURNAME ▶						
DATE ▶						

appropriate. In time, this information may be made available to the public voluntarily, or become available to the public through the Freedom of Information Act. Moreover, other departments and agencies of government may request access to this information pursuant to the Privacy Act of 1974. The information may also be made available in whole or in part to committees or subcommittees of the U.S. Congress.

If you have testified previously with respect to the Three Mile Island accident, it would be useful if you could review any transcripts of your previous statement(s) prior to the deposition.

Thank you for your cooperation.

Sincerely,

/s/

Mitchell Rogovin, Director
NRC/TMI Special Inquiry Group

DISTRIBUTION
TERA
WParler
PNorry
RDeYoung
EKCornell
GFrampton
MRogovin

OFFICE ▶	NRC/TMI	NRC/TMI	NRC/TMI	NRC/TMI	NRC/TMI	NRC/TMI
SURNAME ▶	WParler:kr:mc	PNorry	RDeYoung	EKCornell	GFrampton	MRogovin
DATE ▶	9/ /79	9/5/79	9/5/79	9/ /79	9/ /79	9/ /79

NRC FORM 318 (9-76) NRCM 0240

☆ U.S. GOVERNMENT PRINTING OFFICE: 1979-289-369

SEP 5 1979

MEMORANDUM FOR: William Parler

FROM: E. Kevin Cornell, Staff Director

SUBJECT: DELEGATION OF AUTHORITY TO ADMINISTER OATHS

You are hereby delegated the Commission's Authority to administer oaths for the purpose of taking the deposition of:

Dr. Stephen H. Hanauer, Room P-822, Phillips Building
Dr. Denwood Ross, Room 6715, Maryland National Bank Building

during the period September 25-28, 1979, in connection with the Commission's investigation of the accident at Three Mile Island, Unit 2. This authority is provided to the Commission by Section 161c of the Atomic Energy Act of 1954, as amended, and has been delegated to me via the enclosed memorandum from the Chairman of the Commission. No further delegation of this authority is permitted.

9/5/79
Date

(Signed) E. Kevin Cornell

E. Kevin Cornell
Staff Director
NRC/TMI Special Inquiry Group

Enclosure:
Delegation of Authority memo
fm Chairman Hendrie

OFFICE	NRC/TMI	NRC/TMI	NRC/TMI	NRC/TMI	
SURNAME	WParler:kr:mc	PNorry	RDeYoung	EKCornell	4
DATE	9/5/79	9/5/79	9/5/79	9/5/79	

C
O
P
Y

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
UNITED STATES ATOMIC ENERGY COMMISSION
WASHINGTON, D.C.

Exhibit 1032

July 17, 1969

Honorable Glenn T. Seaborg
Chairman
U. S. Atomic Energy Commission
Washington, D. C. 20545

Subject: REPORT ON THREE MILE ISLAND NUCLEAR STATION UNIT 2

Dear Dr. Seaborg:

At its 111th meeting, July 10-12, 1969, the Advisory Committee on Reactor Safeguards reviewed the proposal of the Metropolitan Edison Company and the Jersey Central Power and Light Company to construct Unit 2 at the Three Mile Island Nuclear Station. A Subcommittee also met to review this project on June 26, 1969. During its review, the Committee had the benefit of discussions with representatives and consultants of both applicants, the Babcock and Wilcox Company, Burns and Roe, Inc., General Public Utilities Corp., and the AEC Regulatory Staff. The Committee also had available the documents listed below.

The plant will be located adjacent to Unit 1 on Three Mile Island near the east shore of the Susquehanna River, about 10 miles southeast of Harrisburg, Pennsylvania. The nuclear steam supply system, engineered safety features, reactor building, and aircraft hardening protection are similar to those of Unit 1, noted in our January 17, 1968, and April 12, 1968, reports. Unit 2 will be operated at a power level of 2452 MWt.

Review of Unit 2 has taken into account the similarities of the Three Mile Island units, new features, updating of the research and development programs, and further evaluations of the site. The review also included matters previously identified that warrant careful consideration for all large, water-cooled power reactors; the Committee believes that resolution of these matters should apply equally to this reactor.

The estimate of probable maximum flood discharge in the Susquehanna River at the site is being revised upwards by the U. S. Army Corps of Engineers and will be larger than had been considered in the design of Unit 1. The applicant has stated that both units will be protected by measures which would assure a safe, orderly shutdown of the reactors in the event of the maximum flood.

C
O
P
Y

C
O
P
Y

The applicant has conducted a test program in support of his proposal to grout the stranded tendons for the containment prestressing system. The Committee believes that adequate grouting can be attained through proper and careful execution of the procedures developed in this program. The applicant has proposed a program of periodic proof testing at 115% of design pressure to monitor the integrity of the containment, which has been designed conservatively to obviate any adverse effects of repeated proof testing at this high pressure. The Committee believes that such a program, involving measurement of deformations and thorough inspection for cracking of the concrete during each proof test, will provide reasonable assurance of the continued integrity of the containment.

Further review is necessary of the research and development being completed for the alkaline sodium thiosulfate spray additive to determine whether the spray systems as proposed need augmentation to achieve required performance in postulated accidents. Provisions will be incorporated in the design of the containment system to permit equipment additions if necessary to ensure limiting the radiological consequences of a loss-of-coolant accident to doses significantly below the 10 CFR 100 guideline values.

The applicant has been considering a purge system to cope with potential hydrogen buildup from various sources in the unlikely event of a loss-of-coolant accident. Additional studies are needed to establish the acceptability of this system and to consider alternative approaches. These studies should include allowance for levels of zircaloy-water reaction which could occur if the effectiveness of the emergency core cooling system were significantly less than predicted. The Committee believes that this matter can be resolved during construction of the reactor.

The Committee reiterates its belief that the instrumentation design should be reviewed for common failure modes, taking into account the possibility of systematic, non-random, concurrent failures of redundant devices, not considered in the single-failure criterion. The applicant should show that the proposed interconnection of control and safety instrumentation will not adversely affect plant safety in a significant manner, considering the possibility of systematic component failure. The Committee believes that this matter can be resolved during construction of the reactor.

The Committee believes that, for transients having a high probability of occurrence, and for which action of a protective system or other engineered safety feature is vital to the public health and safety, an exceedingly high probability of successful action is needed. Common failure modes must be considered in ascertaining an acceptable level of protection. The Committee recommends that a study be made of the possible consequences of hypothesized failures of protective systems during anticipated transients, and of steps to be taken if needed. The Committee believes that this matter can be resolved during construction of the reactor.

C O
P
Y

C
O
P
Y

July 17, 1969

Honorable Glenn T. Seaborg

The Committee recommends that the applicant study possible means of in-service monitoring for vibration or for the presence of loose parts in the reactor pressure vessel as well as in other portions of the primary system, and implement such means as are found practical and appropriate.

The post-accident cooling system must retain its integrity throughout the course of an accident and the subsequent cooling period. The applicant should review the effects of coolant temperature, pH, radioactivity, corrosive materials from the core or other parts of the containment (including stored chemicals), and potentially abrasive slurries. Degeneration of components such as filters, pump impellers, and seals by any of these mechanisms should be reviewed. Particular attention should be paid to potential problems arising from the use of dissimilar metals in these systems.

The Committee recommends that details concerning the adequacy of the design, the material characteristics, quality assurance, and in-service inspection requirements of the main coolant-pump flywheels be resolved between the applicant and the Regulatory Staff. In this connection, and, in general, the Committee continues to emphasize the need and importance of quality assurance, in-service inspection and monitoring programs, as well as conservative safety margins in design.

The Advisory Committee on Reactor Safeguards believes that the items mentioned can be resolved during construction, and that, if due consideration is given to the foregoing, Unit 2 proposed for the Three Mile Island site can be constructed with reasonable assurance that it can be operated without undue risk to the health and safety of the public.

Sincerely yours,

/s/ Stephen H. Hanauer

Stephen H. Hanauer
Chairman

References:
1. Three Mile Island Nuclear Station - Unit 2, Preliminary Safety Analysis Report, Volumes 1-4 (Amendment No. 6, Oyster Creek Nuclear Station, Unit 2, Docket No. 50-320).

2. Amendments 7-10 to Application for Licenses.

3. Metropolitan Edison Company letter dated July 3, 1969.

C
O
P
Y

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

October 22, 1976

Exhibit 1033

Honorable Marcus A. Rowden
Chairman
U. S. Nuclear Regulatory Commission
Washington, DC 20555

SUBJECT: REPORT ON THREE MILE ISLAND NUCLEAR STATION, UNIT 2

Dear Mr. Rowden:

During its 198th meeting, October 14-16, 1976, the Advisory Committee on Reactor Safeguards completed its review of the application of the Metropolitan Edison Company, Jersey Central Power and Light Company, and Pennsylvania Electric Company (Applicants) for a license to operate Three Mile Island Nuclear Station, Unit 2. This project was also considered during a Subcommittee meeting held in Harrisburg, Pennsylvania, on September 23 and 24, 1976. Members of the Committee visited the facility on September 23, 1976. During its review, the Committee had the benefit of discussions with representatives and consultants of the Applicants, General Public Utilities Service Corporation, the Babcock and Wilcox Company (B&W), Burns and Rowe, Inc., and the Nuclear Regulatory Commission (NRC) Staff. The Committee also had available the documents listed below. The Committee reported on the application for a construction permit for Unit 1 on January 17 and April 12, 1968, and for an operating license for Unit 1 on August 14, 1973. The Committee reported on the application for a construction permit for Unit 2 on July 17, 1969.

The Three Mile Island Nuclear Station, Units 1 and 2, is located on Three Mile Island near the eastern shore of the Susquehanna River, about 12 miles southeast of Harrisburg, Pennsylvania. About 2380 people live within a two-mile radius of the site (the low population zone). The minimum exclusion distance is 2000 feet. The nearest population center is Harrisburg (1970 population 68,000).

Several changes have been made to bring the Babcock and Wilcox Emergency Core Cooling System (ECCS) evaluation model into conformance with the requirements of 10 CFR 50.46, and Appendix K to Part 50. Analyses of a spectrum of break sizes appropriate to Three Mile Island, Unit 2 have been completed using the approved B&W generic evaluation model. The results of the analyses for the reactor coolant pump discharge break, believed to be the "worst" break, show maximum allowable linear heat generation rates as a function of elevation in the reactor core ranging from 15.5 to 18.0 kilowatts per foot. Corresponding calculated post-accident peak clad temperatures range from 2002°F to 2146°F. The NRC Staff has identified additional information that it will require to complete its review and the Applicants' submittal is expected by the end of 1976. The Applicants propose to use both in-core and ex-core instrumentation to assure accuracy of measurement of core power distributions. The Committee believes that the proposed monitoring methods may be acceptable, but that an augmented startup program should be employed, and that satisfactory experience at 100% steady state power and during transients at less than full power should be obtained. This experience should be reviewed and evaluated by the NRC Staff prior to operating at up to full power in a load following mode. The Committee wishes to be kept informed.

A question has arisen concerning asymmetric loads on the reactor vessel and its internal structures for certain postulated loss-of-coolant accidents in pressurized water reactors. The Staff has required the Applicants to supply further information in order to complete its assessment of this matter. This issue should be resolved in a manner satisfactory to the NRC Staff.

The question of whether Unit 2 requires design modifications in order to comply with WASH-1270, "Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors", remains an outstanding issue pending the NRC Staff's completion of its review of B&W generic analyses of anticipated transients without scram. The Committee recommends that the NRC Staff, the Applicants and B&W continue to strive for an early resolution of this matter in a manner acceptable to the NRC Staff. The Committee wishes to be kept informed.

Emergency plans have been developed to allow plant shutdown and maintenance of safe shutdown in the event of a maximum probable flood. Such a postulated flood would top the levee surrounding the plant by several feet. Included in the plan is the fastening of water tight steel panels in doorways and other openings of safety related structures. The Committee believes that the details of this plan, particularly relating to re-entry into the station during the post-flood period, need to be more clearly delineated.

The Committee supports the NRC Staff's program for evaluation of fire protection in accordance with Branch Technical Position APCSB 9.5-1, Appendix A, "Guidelines for Fire Protection for Nuclear Power Plants". The Committee recommends that the NRC Staff give high priority to the completion of both owner and Staff evaluations and to recommendations for Three Mile Island Unit 2 and other plants nearing completion of construction in order to maximize the opportunity for improving fire protection while areas are still accessible and changes are more feasible.

The Committee notes that long-term post-accident operation of the plant to maintain safe shutdown conditions may be dependent on instrumentation and electrical equipment within containment which is susceptable to ingress of steam or water if the hermetic seals are either initially defective or should become defective as a result of damage or aging. The Committee believes that appropriate test procedures to confirm continuous long-term seal capability should be developed.

The Committee recommends that further review be made of the battery supplied DC power system to assure that non-essential loads do not interfere with its safety function. The Committee recommends that further review be made to assure no unacceptable effects such as release of hydrogen into the plant can occur from the failure of a hydrogen charging line. The Committee also recommends that studies be made to assure that failure of an instrument line cannot cause plant controllability problems of significance to public safety.

The management organization proposed by the Applicants to delineate the safety related responsibilities of the off-site and on-site personnel of the Three Mile Island Station left open questions as to how these responsibilities are to be discharged during normal working hours and during evening, night, and weekend shifts. This matter should be resolved to the satisfaction of the NRC Staff.

The NRC Staff is still reviewing various issues related to accidents leading to loss of fluid in the steam generator secondary side, such as steam line breaks. The Committee wishes to be kept informed of the resolution of these issues.

The Committee recommends that, prior to commercial power operation of Three Mile Island Unit 2, additional means for evaluating the cause and likely course of various accidents, including those of very low probability, should be in hand in order to provide improved bases for timely decisions concerning possible off-site emergency measures. The Committee wishes to be kept informed.

The Committee believes that the Applicants and the NRC Staff should further review the Three Mile Island Nuclear Station for measures that could significantly reduce the possibility and consequences of sabotage, and that such measures should be implemented where practical.

Other generic problems relating to large water reactors are discussed in the Committee's report entitled "Status of Generic Items Relating to Light Water Reactors: Report No. 4", dated April 16, 1976. Those problems relevant to the Three Mile Island Station should be dealt with appropriately by the NRC Staff and the Applicants as solutions are found. The relevant items are: II - 1, 2, 3, 4, 5, 6, 7, 9, 11; IIA - 1, 4, 5, 6, 7, 8; IIC - 1, 2, 3, 4, 5, 6, 7.

The Advisory Committee on Reactor Safeguards believes that, if due regard is given to the items mentioned above, and subject to satisfactory completion of construction and pre-operational testing, there is reasonable assurance that Three Mile Island Nuclear Station, Unit 2 can be operated at power levels up to 2772 MWt without undue risk to the health and safety of the public.

Sincerely yours,

Dade W. Moeller

Dade W. Moeller
Chairman

References

1. Three Mile Island Nuclear Station, Unit 2 Final Safety Analysis Report (April, 1974) with Amendments 1 through 44.

2. Safety Evaluation Report (NUREG-0107) related to operation of Three Mile Island Nuclear Station, Unit 2, dated September, 1976.

Exhibit 1034 Bailey 417

REPORT TO THE ATOMIC ENERGY COMMISSION
ON THE REACTOR LICENSING PROGRAM

by the

INTERNAL STUDY GROUP

June 1969

<u>CONTENTS</u>

PREFACE

On July 8, 1968, the Atomic Energy Commission announced plans for an internal review of its regulatory program to help assure that procedures keep pace with the rapid expansion of the nuclear industry. In this review, designed to be primarily technically oriented, the present process for the licensing of power reactors was to be examined from the standpoint of efficiency in the discharge of regulatory responsibilities and compatibility with the commercial arrangements by which nuclear plants are purchased, designed, constructed and operated. The purpose of the review was to recommend possible improvements in the licensing process, and to determine whether further detailed Commission study in any areas would be desirable.

To conduct this review, the Commission named an Internal Study Group drawn from the three principal components of the AEC regulatory system - the staff operation headed by the Director of Regulation (the regulatory staff), the Advisory Committee on Reactor Safeguards (ACRS) and the Atomic Safety & Licensing Board Panel (ASLBP). Members appointed to serve on the Internal Study Group were:

Harold G. Mangelsdorf, Chairman
(Member, ACRS)

Warren E. Nyer, Vice Chairman
(Vice Chairman, ASLBP, 1968)

Edson G. Case
(Director, Division of Reactor Standards, AEC)

John W. Crawford, Jr.
(Assistant Director, Division of Reactor
Development and Technology, AEC)

David B. Hall
(Member, ASLBP; Chairman, ACRS, 1963)

Stephen H. Hanauer
(Chairman, ACRS, 1969)

Peter A. Morris
(Director, Division of Reactor Licensing, AEC)

Carroll W. Zabel
(Chairman, ACRS, 1968)

Marcus A. Rowden, Assistant General Counsel for the AEC was appointed to serve as legal counsel and Ray G. Smith of the AEC's Division of Reactor Standards was selected as Technical Secretary.

The Internal Study Group met at approximately bi-weekly intervals during the period between July 1968, and April 1969. Discussions were held with representatives of publicly and privately owned utilities, reactor manufacturers, architect-engineers engaged in the design and construction of nuclear power plants, and various industry associations. Discussions were also held with Federal Aviation Administration representatives, two members of an earlier regulatory review panel and senior representatives of the AEC regulatory and other staff.

The Internal Study Group has arrived at a number of conclusions, and has developed some related recommendations. The purpose of this report is to present these conclusions and recommendations and to discuss the reasoning behind them.

II. INTRODUCTION

The Internal Study Group undertook its review of the reactor licensing process with a view toward making suggestions for ways to improve the process and its effectiveness in protecting the health and safety of the public, while at the same time minimizing the problems faced by the nuclear industry and the regulatory groups. In addition to specific aspects of the licensing process, the Group considered the general questions of (1) the adequacy of the protection of the health and safety of the public and (2) whether regulatory procedures and requirements have adversely affected the development of the industry.

The Group concludes that the health and safety of the public has been adequately protected. At the end of 1968, 17 licensed power reactors had been built and operated, nine of which continue in routine operation, with an accumulated experience of 88 reactor years. No member of the public has been exposed to radiation levels above permissible annual limits as a result of the operation of these licensed power reactors. Although this experience does not provide conclusive proof of safety, it does provide some indication that the health and safety of the public is being protected. The general consensus among the industry representatives who talked with the Study Group was that there is a high degree of conservatism in nuclear plant designs and in safety reviews, and that this conservatism is at least as great as that of most other major industrial activities. It was also agreed that this conservatism has contributed substantially to the good safety record of the nuclear industry and that it is not out of proportion to the needs of the industry. The Study Group concurs in this view.

The groups and individuals who talked with the Study Group were asked if they believed the regulatory bodies had required unnecessary or superfluous safety features. Few examples were cited of safety requirements that were believed not to be needed. A few persons expressed the belief that future experience might show that some systems need not be required; however, the principal concern was not with the requirements themselves, but with the added complexity and, perhaps, excessive redundancy that seemed to result and the uncertainty as to the safety requirements and the timing for their imposition. In general, the consensus of the industry representatives - concurred in by the Study Group - was that safety feature requirements have not been out of proportion to the need for the protection of the health and safety of the public.

There was also general agreement that the licensing review process at the construction permit stage has not been a limiting item in the time schedule for the construction of plants, although it could become so in the future. In the latter connection, a major problem considered by the Group, to which some of its specific recommendations are related, is the lack of correspondence in timing of decision points in the current licensing review process with decision points in the process of industrial procurement, construction and initial operation of nuclear plants. This lack of correspondence, together with uncertainties in regulatory requirements, has resulted in some hardship and frustration to some elements of the industry and could become even more troublesome as the market for nuclear power expands.

The problem mentioned most by industry representatives was uncertainty and instability in regulatory requirements. Utilities faced with decisions on the addition of generating capacity have not been certain of ultimate licensing requirements at the time of their selection of the type of nuclear power units to be installed and when they contracted for those units. There have been related increases in costs and changes in plant scheduling and manpower requirements which were not anticipated when utility selection and contracting decisions were made. Many of these unanticipated changes were the result of safety requirements imposed by the regulatory groups to maintain adequate margins of safety consistent with increases in reactor size and power density. Neither the industry nor the regulatory groups had foreseen the extent of the provisions that would be needed to maintain these safety margins.

In the long run, the greater stability and predictability of regulatory requirements which both industry and the regulatory groups seek will depend on the development of comprehensive safety criteria, codes and standards. While there has been considerable progress in that direction by both the Commission and industry, more needs to be done - a matter dealt with elsewhere in this report.

As the designs for the newer and larger nuclear plants are evolving and as more comprehensive regulatory safety criteria are being developed, it is especially important that all groups involved in the review process, and also those involved in the conduct of research and development programs directed toward resolution of potential safety problems, maintain effective communication with each other. The Study Group notes that the effectiveness of this communication has steadily improved. In particular, the Group supports the current joint efforts at the staff level within the Commission to define regulatory needs and to orient Commission-supported research programs toward resolution of those needs on a timely basis. These efforts should be continued and expanded to include active participation by the nuclear industry, particularly by utilities.

The Study Group discussed at some length the continuing problem of maintenance of an effective regulatory process in an industry marked by a rapidly developing technology and large increases in the number of applications to be processed. The Study Group believes that the AEC regulatory staff should continue to be the only regulatory body to perform a complete technical review of each reactor application. The regulatory staff should have sufficient strength - in manpower and other resources - to carry out in a timely fashion the activities necessary to assure that the regulatory process provides effective protection to the health and safety of the public.

Detailed discussion of many of these points will be found in the following sections of this report.

III. CONCLUSIONS AND RECOMMENDATIONS

A. Development of Regulatory Criteria and Standards Relating to Safety

The lack of a comprehensive set of regulatory safety criteria and industry codes and standards relating to the safety of nuclear power plants contributes to the uncertainty concerning regulatory requirements and to the length of time required to conduct regulatory safety evaluations.

CONCLUSIONS AND RECOMMENDATIONS

1. Current efforts to develop and implement comprehensive regulatory safety criteria and industry codes and standards relating to the safety of nuclear power plants should be intensified consistent with the critical importance of such criteria codes and standards for improving the regulatory process and benefiting the nuclear power industry.
2. There is an urgent need for substantially increased participation in and support of these efforts by all segments of the nuclear industry, especially the utilities.
3. The ACRS should expand its participation in the development of regulatory criteria and standards relating to safety.

DISCUSSION

The Study Group believes that significant benefits to the nuclear industry would result from the development and implementation of comprehensive regulatory safety criteria and of industry codes and standards relating to the safety of nuclear power plants. Such criteria, codes and standards would contribute measurably to industry understanding of licensing requirements and would, at the same time, furnish an improved means for demonstrating that the necessary requirements have been met. Their use would result in better definition of the information to be supplied in license applications and so aid in reducing significantly the time required for regulatory reviews. In addition, the Group believes a greater effort by both industry and the AEC to describe the technical bases for safety requirements would be beneficial.

The Study Group in its discussions with industry representatives found substantial recognition of the need for, and importance of, hastening the development of regulatory safety criteria and of industry codes and standards relating to safety. The Group found that the organizations affected are strongly interested in reviewing proposed criteria, codes and standards before they are put in effect. It was less clear that such organizations recognize the importance of participating in and actively supporting current standards-making efforts within the nuclear industry.

The Commission has been strengthening its efforts on the development of regulatory safety criteria, codes and standards, including cooperative efforts with professional standards groups, the supplier industry and the utilities. The nuclear industry, through the United States of America Standards Institute, professional societies and industry associations, has also taken some strengthening measures to develop codes and standards. In addition, some companies have individually recognized their responsibilities and are actively supporting these efforts. However, despite the significant progress that has been made in the last few years, the Study Group believes that the rate of accomplishment by the Commission and the industry has not been fast enough to meet the needs of the rapidly developing industry.

While more technical information is needed before development of comprehensive regulatory criteria can be completed, the Group believes that the basic organizational structures and technical capabilities for developing the needed industry safety codes and standards already exist. The urgent requirement is for all segments of the nuclear industry to recognize their vital interest in supporting such efforts and to implement that recognition through aggressive leadership and the furnishing of knowledgeable personnel on a high priority basis.

The Group is aware that the procedures associated with developing and promulgating regulatory safety criteria and industry codes and standards have, traditionally, been time-consuming. This postpones their availability for use. The effect of this traditional pattern is compounded by the time required to construct plants, with the result that current efforts will not be seen in operating nuclear power plants for many years. The Group believes that measures to reduce these delays should be taken by the regulatory groups, by standards-making organizations and by the nuclear industry.

While emphasizing the responsibility the nuclear industry has in developing codes and standards relating to safety, the Group is aware of some of the difficulties that are involved. These difficulties derive from many factors, including procedures which require near unanimous agreement to establish such standards or to modify them. In view of the nature of these factors, it is not realistic to expect that industry's efforts can result in safety codes and standards which alone will be adequate to protect the public. Accordingly, there will continue to be a need for the Commission to develop and promulgate supplementary regulatory requirements. However, to the degree that industry succeeds in adopting codes and standards which meet safety requirements, the need for additional requirements imposed by the Commission will be reduced.

B. Differing Views on Reactor Safety Requirements

There are differing views among those in the nuclear industry, the regulatory groups and others, as to how the safety of nuclear power plants can best be provided. There are differences of opinion on the degree of reliance which should be placed on the reactor system itself and on engineered safety features; the number of such features required; and the kinds of failures to be considered. There are differences of opinion on whether, and to what extent, trade-offs can be made among the various safety elements. For example, can there be a reduction in the extent of duplication and layering of systems designed to limit the consequences of accidents if it is known that an effective quality assurance program has been applied throughout the design and construction of the plant? Alternatively, can the performance specifications for reactor containment be reduced if there is adequate assurance that fuel melting cannot occur?

RECOMMENDATION

The Commission should adopt the policy that the greatest emphasis and priority be placed on the application of quality assurance to the design, construction and operation of nuclear plants so as to achieve the exacting level of safety required.

DISCUSSION

The Study Group observes that the primary objective of the nuclear power industry is to build and operate safe, reliable and economically attractive generating plants. The Group is convinced that attainment of this objective requires rigorous application of quality assurance procedures in the broadest sense.

The achievement of an adequate level of safety for nuclear power plants is generally recognized to require defense-in-depth in the design of the plant and its additional engineered safety features. The degree of emphasis on defense-in-depth in the nuclear field is new to the power industry.

In seeking reliability of safety systems, there has been much attention in the nuclear field to redundancy, diversity and quality control. As a result of the evolution of designs, and the large number of new orders for nuclear plants, questions have been raised regarding the proper balance among back-up systems with respect to the requirements of basic plant design.

The Study Group endorses the defense-in-depth concept, but believes that the greatest emphasis should be placed on the first line of defense, i.e., on designing, constructing, testing, and operating a plant so that it will perform during normal and abnormal conditions in a reliable and predictable manner. This assurance of quality is obtained only if safety requirements are clearly and adequately defined, plant designs meet these requirements without excessive complexity, construction is in accord with design, and operation and maintenance assure continuing conformance with safety criteria. The need for greater emphasis on quality assurance is supported by recent experience which has revealed a number of defects in reactor construction and deficiencies in meeting design objectives that have required correction in plants currently under construction.

A number of factors are included in the recommended emphasis on quality assurance, all of which need attention to achieve the overall goal. Among these are independent reviews of design, construction, tests and operation; deliberate use of inherent safety features; provision for effective inspection, maintenance and surveillance; accurate records; and performance evaluation.

The Group considers that industry has not demonstrated sufficient recognition of the contribution to safety that can be made by designing, constructing, testing and operating a plant so that it will perform during normal and abnormal conditions in a reliable and predictable manner. Consequently, greater attention should be given by the industry to establishing the strong quality assurance programs that experience has shown are needed to achieve this kind of performance.

The Study Group believes that nuclear power plants designed, built, tested and operated in a disciplined manner with exacting standards of quality will provide an adequate level of safety. Nevertheless, abnormalities, deviations and accidents may occur; and with no operating experience with the large reactors of new design, the Group does not believe that current requirements for engineered safety features are excessive or that trade-offs should be made at this time among the various elements of design contributing to defense-in-depth. In this regard, most of those to whom the Group talked could offer no suggestion for elimination of the systems now provided.

There was universal support for strong quality assurance programs among those to whom the Group talked. There is, however, a wide variation of understanding and experience in this area. The Group concurs in the definition of quality assurance set forth in the "Nuclear Power Plant Quality Assurance Criteria," being developed for issuance by the Commission:

> "Quality assurance comprises all those planned and systematic actions necessary to provide adequate confidence that a structure, system, or component will perform satisfactorily in service."

The term is used in the broad sense of applying quality assurance throughout all phases of the design, construction, testing and operation of a nuclear power plant. It includes quality control, which comprises those actions related to the physical characteristics of a material, component or system and which provides a means to control quality to predetermined requirements.

In view of the wide variation in understanding of quality assurance and the need for increased attention to this matter, the Group believes it would be useful for the Commission to adopt the policy of putting first priority and emphasis on quality assurance, as earlier defined, in providing nuclear plants with an adequate level of safety.

In sum, the Group believes that greater emphasis should be placed on providing sound quality assurance programs in the nuclear industry and that there should be no present reduction in the requirements for back-up or consequence-limiting safety features in current designs for water-cooled nuclear power plants.

C. Safety Research as Related to the Licensing of Power Reactors

Consistent with the Commission's two stage licensing process, construction permits for large water-cooled power reactors have been issued on the basis that there is reasonable assurance that safety questions requiring research and development will be satisfactorily resolved prior to completion of the proposed facilities. Because of the large number of these plants scheduled to begin operation in the next few years, special attention must be directed to assuring that the required research is being conducted and that the results will be available when needed.

RECOMMENDATIONS

1. Applicants, reactor designers and the regulatory groups should continue to refine and formalize the existing practice of identifying at the construction permit stage for each nuclear power plant the safety issues requiring resolution by research, and the scope and schedule of programs expected to provide the information needed to resolve these issues.
2. Present AEC efforts to document and review Commission and industry-sponsored safety research programs to determine whether these programs are adequate for timely resolution of safety issues for large water-cooled nuclear power plants should be continued and expanded

to include active participation by reactor designers and utilities.

3. If necessary research programs are not being conducted, or are not sufficiently responsive to the identified needs, alternative courses of action should be developed and implemented by the AEC and the nuclear industry.

DISCUSSION

Both the Commission and the industry sponsor nuclear safety research programs to support the development of power reactors. Historically, the AEC has financed much of the safety research for water-cooled power reactors and it continues to support these safety research programs. The large number of construction permits for these power reactors which have been issued in the last several years does not imply there is a decreasing need for water reactor safety research. Rather, because these construction permits were issued on the basis that planned research programs would resolve certain safety questions related to these reactors and because new questions have resulted from the increases in reactor power level and power density, there is an increasing need for safety research. As a result, the combined AEC and industry research program on safety questions related to water-cooled power reactors continues to grow.

It is difficult to distinguish safety research necessary for the licensing of individual power reactors from basic safety research that increases the understanding of safety-related technical questions. There is some tendency to classify in the basic category all research needed to resolve the safety questions identified for large water-cooled nuclear power plants and to place complete responsibility on the AEC for conducting the necessary programs. An opposing view considers the technical questions to be related only to specific plant designs and believes that AEC financial support for water reactor safety research should be significantly curtailed, if not eliminated. Whatever the view and irrespective of who finances the programs to develop the information, it is indisputably the licensee's responsibility to provide the information necessary to resolve the technical safety questions related to his nuclear power plant.

Most of the present safety research effort is directed toward providing information concerning potential accidents having very low probabilities of occurrence. Analyses have shown that the safety features provided in current designs of water-cooled power reactors are adequate to protect against these accidents. While the Study Group believes it is reasonable for some nuclear power plants to begin operation with the assurance of adequacy of safety features dependent on analyses, it is important that these analyses be confirmed in a timely fashion by the results from planned research programs.

The first necessary step to this end is to identify clearly for each plant at the construction permit stage the technical questions requiring research, and the scope and scheduling of programs expected to provide the information needed to resolve the questions. The Study Group is aware that, in recent licensing cases, efforts have been made to document not only the technical issues for the particular power reactors and the research programs necessary to provide information to resolve those issues, but to document also the schedules of the necessary research programs. The Group recommends that such efforts be further systematized so that licensees, regulatory groups and those responsible for conducting research can more clearly understand what specific information will be required prior to operation of power reactors and the timing necessary for developing this information.

A second step to assure that research is oriented to meet safety and licensing requirements is to document and review periodically the existing and planned programs. The Study Group notes that efforts in this regard are underway by the AEC's development and regulatory staffs. The Group further notes that increased communication between the Commission's regulatory and development staffs has resulted in better coordination of the AEC-sponsored research programs with regulatory needs. These staff level actions have been fostered and encouraged by the AEC's Steering Committee on Reactor Safety Research.

The Study Group believes there should be increased participation by the nuclear industry, particularly by utilities, in current AEC efforts to relate the research programs in water reactor safety to the requirements and schedules of the licensing process. Discussions, at both management and staff levels, should be arranged among appropriate AEC, reactor designer and utility personnel who are conversant with industry research and nuclear power plant licensing and safety. Through better appreciation of each other's problems, both technical and financial, and by frank discussion of the technical safety issues, a better definition of the necessary scope and schedule of the safety research programs can be developed. Possible courses of action if these needs are not being satisfied can also be determined.

Closer cooperation between AEC and industry on safety research would improve the basis for determining which of the needed safety research programs should be financed by the nuclear industry and which by the AEC. Development of appropriate financial arrangements at this time, when the AEC is still sponsoring a major portion of the water reactor safety research program, will ease the inevitable transition to the time when industry must initiate and fund most of this program.

D. Relative Emphasis on Large and Small Accidents

The Study Group considered the problem of whether detailed consideration of a few serious postulated accidents is diverting effort from needed study of less serious, more probable malfunctions.

CONCLUSIONS AND RECOMMENDATIONS

1. It remains necessary to consider, in safety reviews, a wide variety of expected transients and postulated accidents.
2. The design basis accidents presently used in the safety evaluation of large water-cooled power reactors should not be changed until convincing technical evidence is available that the change is justified.
3. An integrated engineering approach is needed; safety features added to cope with one malfunction should be engineered so as to not unduly increase the probability or consequences of another malfunction.

DISCUSSION

Early safety reviews included postulated complete reactor failure and an all-enveloping containment sufficient to maintain off-site exposure at a tolerable level and thus to protect the public. All other possible accidents were considered to have contained consequences less severe than those of the maximum accident; therefore, the containment provided protection to the public for small as well as large accidents. The increase in the size and complexity of reactors since that time has required development of a system of engineered safety features which would operate in accident situations to prevent fuel failure and melting, to remove afterheat, and to cope with a radioactive, hydrogen-rich containment atmosphere in order to provide containment or confinement of radioactivity for the protection of the public.

The regulatory system for safety reviews has evolved from one based on consideration of a single worst accident into one which considers a spectrum of expected transients and a number of postulated malfunctions and design basis accidents. For the larger reactors, containing the worst accident considered credible does not insure that all credible accidents would be contained. Since it is not permissible in the case of large reactors to concentrate safety reviews on the worst accidents and to ignore the lesser ones, a spectrum of accidents is considered.

Which postulated accidents should be used as the design basis for reactor safety? In the absence of wide experience with reactor accidents, calculation and judgment must be substituted for such experience. It has been suggested that the design-basis accidents presently used should be revised to reflect a more nearly consistent and mechanistic view of what would actually happen. The Group believes that sufficient knowledge is not available to justify such a revision, and that current use of the non-mechanistic set of design-basis accidents presently employed provides a needed safety margin to allow for unknown factors. Changes in these design basis accidents should be made only when justified by convincing technical evidence.

In designing protective systems and safety features to deal with postulated malfunctions and transients, an integrated engineering approach is needed to prevent interference of one safety feature with another, or with normal operation. A device added to increase safety in some postulated situation should not unduly increase the probability or consequences of any other malfunction. This possible result is a criticism the Group heard of the present design-basis accidents, i.e. that detailed attention to serious, highly improbable postulated accidents might result in such complex systems that overall safety might be decreased. Neither the industry representatives heard by the Group, nor the Group itself, believe that this decrease in safety has actually occurred; and no examples were suggested of safety features that decreased overall safety. The Study Group believes, however, that continued attention is required to the engineering of safety features in a consistent, disciplined way so that safety is in fact increased by their installation.

In this connection, it seems worth noting that the reliability required of a safety device depends both on the probability of need for its function and the consequences of its failure to function when needed. Implicit in this statement is the knowledge that risk cannot be made exactly zero, but that an extremely low, acceptable value must be maintained. Postulated events of sufficiently low probability need not be protected against, since the risk from them is negligible. For serious potential accidents of low, but not negligible, probability of occurrence, protective systems with good reliability are required. Situations for which the anticipated rate of occurrence is relatively high (say, once every few years) require protective systems of extremely high reliability in order to reduce the risk to an acceptably low value. These more frequent events — expected transients — play an important role in the assessment of the overall risk and may determine the reliability requirements of reactor protective systems. The Group believes this matter warrants further consideration.

Attention should be directed toward expected transients and non-catastrophic malfunctions for another reason: they provide potentially useful indicators of incipient safety problems in an operating reactor. The rate of such incidents, and also of malfunctions in the protective systems and engineered safety features, should remain at a tolerably low level, consistent with design expectations. Discovery of a malfunction rate higher than that reasonably expected — in particular, of any upward trend in the rate with time — should be considered evidence that something is amiss. For example, it is beside the point that an abnormally high rate of unneeded reactor trips is in the safe direction. Such a circumstance is a symptom of trouble in ~~the~~ protection system which may include concealed changes adverse to the functioning of the system. For this reason, the continuing surveillance of incidents and malfunctions discussed in Section III.I of this report is important to maintaining the availability of safety devices to perform their functions if needed.

E. Quantification of Safety

It has been suggested that a more quantitative approach be used in the evaluation of risks associated with nuclear power plants both to attempt to establish overall risks and to provide techniques for comparative studies of safety systems. Such an approach, if it could be realized, would assist in reducing uncertainties in the licensing process, particularly in areas which have been criticized for lack of clear, consistent requirements. The Study Group considered whether and to what extent the safety evaluation process can be quantified.

CONCLUSIONS AND RECOMMENDATIONS

1. With existing techniques and knowledge, the total risks to the public from nuclear power plants, although very small, cannot now be meaningfully expressed in numerical terms.
2. Quantification techniques do show promise as a tool in comparative safety evaluation.
3. Efforts should be made to improve the collection of data needed to evaluate the reliability and causes for failure of safety-related systems in nuclear plants. A cooperative effort by the AEC and the nuclear industry, particularly the utilities, probably will be required to achieve such a program.

DISCUSSION

Two fundamental questions are involved in making safety evaluations for a nuclear plant:

1. How much safety do we need?

2. How much safety do we have?

The answer to the first question is an evaluation of the degree of risk that should be accepted. It is inescapably a policy decision, even though the intriguing possibility is being raised that it may be expressed quantitatively in comparison to risks that have been and are being accepted by the public.

The answer to the second question is an evaluation of the risk that is being taken (presumably measured against an answer to the first question). Since it deals with hardware rather than with judgments, it has the possibility in principle of being made on a more quantitative, objective basis. Clearly, if this possibility could be realized, many of the uncertainties in the safety evaluation process would be reduced.

Historically, acceptable levels of risks for activities in society have not been established a priori, but have emerged in the form of acceptable practice (rather than as quantitative evaluations) over a period of time long enough to observe the interplay of costs, benefits and risks.

Primarily because of the risks involved in the low-probability, large-consequence accidents, the nuclear power industry and the regulatory bodies have followed a different course. They have diligently attempted to consider hazards and to apply preventive measures prior to undergoing actual accident experience. In so doing, they have so far eliminated, and hopefully will continue to prevent, the empirical accident experience that has in the past provided the basis for evaluation of actual risk and for determination of the socially acceptable level of risk. There are two important consequences of this circumstance:

1. Estimation of the actual total risk of nuclear power plant operation will be based only on extrapolation of experience data with small-to-moderate accidents and near-accidents. Neither the data nor the conceptual framework now exists or may be attainable for such extrapolations.
2. The acceptable level of risk -- "How much safety do we need?" -- will not be derivable from experience and will be a policy decision.

The answer to the second question -- "How much safety do we have?" -- also involves evaluations not empirically determined. But, in principle, an evaluation can be made. Such evaluations are subject to two basic limitations. First, no certainty exists that all failure modes are recognized, and thus the evaluation may not be conservative. Second, and more basic to the usefulness of the approach, is the lack of probability information of the required detail and accuracy. The availability of information does not appear adequate to permit a meaningful evaluation of total risk.

Further development of techniques for comparative evaluation of risk appears to have promise of beneficial results and should be encouraged. Moreover, even with relatively sparse and imprecise failure data, the existing methodology can be of value in influencing basic design approaches or in comparing performance of subsystems. If properly developed and applied, these techniques might be used to:

1. Compare alternate safety systems and components of engineered safety systems.
2. Measure the relative protection provided against several postulated accidents to help decide which should receive the most attention.
3. Decide if the problems caused by the additional complexity from adding a safety system outweigh the advantages of that system.
4. Measure on a uniform basis the relative gain in safety provided by an additional safety feature.

The nuclear industry and the regulatory groups have not used these quantification techniques in as systematic a way or to the degree they are used in some other industries. The Study Group believes that greater use should be made of these techniques and the development and application of these techniques for comparative analyses by the nuclear industry and by the regulatory groups should be encouraged.

Application of these techniques is dependent upon the availability of adequate data on failure rates and modes. Presently, only gross failures are reported. While the lessons thus learned are invaluable, particularly in identifying previously unsuspected failure modes, much more data is needed. Protective systems and engineered safety features are tested regularly; and compilations of test data -- successes as well as failures -- are a largely untapped source of failure-rate data. It is the utilities that are vital to such a program, since they operate the plants and collect the data. Moreover, it is the utilities who eventually benefit, in enhanced plant availability as well as safety, when lessons learned from failures and reliability studies are fed back into new designs and criteria.

While the proper use of quantification techniques may be helpful, a note of caution should be sounded concerning their misuse. The Study Group believes these techniques should be used as a tool in achieving a sound engineering design. To rely on the use of these techniques as a substitute for or at the expense of a disciplined engineering approach to design with an associated strong quality assurance program would be a misuse of the techniques and could result in a decrease in overall safety.

Successful attempts to quantify safety appear to be limited presently to comparative studies. It is not clear, however, what success might be expected from additional development of the technique and the possibility exists that total risk evaluation may be feasible in the future. In any event, there have been only limited attempts to date at systematic examination of the data requirements for meaningful evaluation, or of the feasibility of alternate approaches.

The Study Group believes such a systematic examination should be made.

In summary, the Group believes that development should be continued on techniques for the quantitative assessment of risk. However, before such techniques will become a practical tool in evaluating overall reactor safety, much work remains to be done in the following areas:

1. Extrapolation from experience with small accidents to quantitative judgments regarding potential serious accidents.
2. Identification of potential failure modes.
3. Development of information on failure rates of equipment and probabilities of postulated accidents.
4. Establishment of an acceptable level of risk.

F. Degree of Standardization and Imposition of Additional Safety Requirements

As proposed reactors have become more nearly alike, regulatory requirements have tended to become more stable. Nevertheless, in a number of cases, safety questions not previously identified have arisen and their resolution has caused delay and increased cost.

A proposed different approach to reactor licensing would be certification of a reactor design and plant safety features outside the context of individual license application reviews. Duplicate plants could then be licensed without extensive review, except for site-related factors. Changes in the certified designs would be considered in a manner similar to the original certification.

Consideration of the value of a certification system requires, among other things, an evaluation of the extent to which current designs of large water-cooled nuclear power plants have become standardized and the degree to which the benefits of standardization can be realized within the present framework of the licensing process.

RECOMMENDATIONS

1. Greater advantage of the current degree of standardization in reactor and plant design should be taken by applicants and the regulatory groups within the present framework of the licensing process in order to realize more of the benefits of this standardization.
2. A formal system for certification of details of reactor and plant design features outside the context of individual

license application reviews should not be adopted by the Commission at this time.

DISCUSSION

There appears to be a considerable degree of standardization by each major supplier in the conceptual designs and the nuclear steam supply systems for current large water-cooled nuclear power plants. There is less standardization, and the technology seems less well developed, in the design of systems, such as emergency core cooling systems, that interface with the nuclear steam supply system.

There is even less standardization in the preliminary design of other engineered safety features for these large nuclear power plants, such as containment, fission product removal systems, and emergency power systems. Factors that hinder their standardization are (1) these features are site-related and thus subject to more variation; (2) they are usually designed by architect-engineer firms, which are more numerous than the companies designing nuclear steam supply systems; and (3) the utility influence on these plant design features is more pronounced.

There has been considerable discussion within the nuclear industry regarding methods for taking advantage of the trend toward standardization in the design of water-cooled power reactors. The Study Group believes that some gains in this direction are evident now and that more of the benefits of the current degree of design standardization can be realized within the framework of the present licensing process. For example, the present regulatory practice of conducting a single safety review for the identical design features of twin nuclear power plants at one site could be extended to cover identical design features of all plants of the same class, taking into account only the different interaction problems and site considerations, and any new safety-related information. The cooperation of applicants proposing duplicate designs is needed, since obtaining the benefits of such a procedure would require clear identification of features and their design bases which are the same as those accepted for a previously reviewed plant. The Group believes there is a potential in greater use of such an approach for considerable savings in regulatory review time.

The Commission announced its willingness in December, 1964, to conduct informal reviews and evaluations of power reactor systems or major components in advance of the formal filing of an application. This procedure has been used successfully on a number of occasions, with varying degrees of examination. Reviews have ranged from initial, informal reactions of the regulatory staff to detailed safety evaluations by both the staff and ACRS. Such reviews, conducted under present procedures, can provide some of the benefits hoped to be achieved by a formal certification process, such as the one discussed later in this section.

The Study Group endorses the proposed changes in licensing regulations concerning provisional construction permits developed by the Director of Regulation and believes these changes will permit greater advantage to be taken of the current degree of standardization in water power reactors. If these changes are adopted, the extent to which specific reactor and plant features are approved by the regulatory groups at the construction permit stage will be more clearly defined, and modifications to the approved design of these features will not be imposed by these groups at the operating license stage unless substantial additional protection, which is required for the public health and safety, would be provided.

Another method which has been proposed to take greater advantage of the current degree of standardization is for the AEC to adopt procedures for approving (certifying) the design of a specific type or portion of a nuclear power plant outside the context of an individual license application. This proposal would provide for establishment of joint AEC-reactor designer groups, apart from any license application proceeding, to identify all the accepted safety design features of a standard reactor and plant design. The proposal provides that each team would then define and set forth in a document all the characteristics and bases of these accepted features which are important to safety. The resulting documents would contain enough details concerning these features so that if the document were included as part or all of subsequent construction permit applications, the features described could be approved without further review by the regulatory groups. This document could also be used at the operating license stage to justify acceptance of the certified design features upon showing that they had been built in accordance with its provisions.

The most important potential advantage of this proposal i- the rapidity which it appears to provide for converting specific decisions made by regulatory groups into a basis that can be applied generally to subsequent licensing reviews of individual applications. The suggested procedure would achieve its purpose primarily by systematizing and organizing the steps in the licensing review process in such a manner that general applicability could be derived from regulatory decisions.

There are several difficulties with this proposal. To begin with, one of the principal premises of the proposal is that prior acceptance of design features of facilities licensed for construction can be translated into general approval of safety features. This would be difficult at the present time, because of the limited number of detailed final designs that have been reviewed, and because of the need to complete research and development programs substantiating design adequacy and the need for confirmatory operating experience.

There are other disadvantages to the certification approach. The certification would represent an agreement on safety-related design aspects between the AEC and the reactor designer, rather than the reactor operator-owner. Thus, this approach would depart from the underlying philosophy of present licensing procedures which places responsibility for safety on the reactor operator. Some of the utilities who met with the Group indicated a reluctance to accept a certification type arrangement unless they could become active participants in the discussions regarding acceptability of specific reactor design features.

By enlarging these discussions to include any or all utilities, complications would be introduced in establishing priorities, in obtaining agreement of all parties and in reaching timely decisions concerning the acceptability of reactor design features.

It appears to the Study Group that formal adoption of certification procedures by the AEC might be more useful and practical in the future than at present. It remains to be seen whether there will be substantial standardization of safety features which will encompass all areas of design, including containment and other site-related features. Further, the results of operating experience with the larger power reactors and of research and development programs, such as those concerning the effectiveness of presently designed emergency core cooling systems, would be available for consideration at that time. In the meantime, the Group believes that further advantage of any standardization of the design of water power reactors can be realized by applicants and the regulatory groups within the framework of the present licensing process.

G. Criteria for Deciding When to Backfit After Issuance of a Construction Permit

The imposition of additional safety requirements after issuance of a construction permit (backfitting) has been dealt with on a case by case basis. While this approach permits maximum flexibility, it also creates considerable uncertainty for licensees. Criteria would be helpful in reducing this uncertainty.

RECOMMENDATION

The Study Group endorses proposed changes in the Commission's regulations developed by the Director of Regulation which will provide that additional safety requirements for a nuclear power facility for which a construction permit has been issued will be imposed by the Commission only if it finds that such action will provide substantial additional protection which is required for the public health and safety.

DISCUSSION

Most industry representatives with whom the Study Group talked criticized the present practice concerning backfitting since it has led to uncertainty after issuance of a construction permit as to what safety features a licensee may have to add or modify in order to receive an operating license without delay.

The Study Group believes that proposed changes in the Commission's regulations concerning backfitting will alleviate some of this uncertainty. The proposed amendment will make it clear that additional safety requirements will be imposed by the Commission after issuance of a construction permit only if it finds that such action will provide provide substantial additional protection required for the public health and safety. The amendment will not affect licensee responsibility for evaluating significant new information developed as a result of experience with design, construction, testing and operation of a reactor or as a result of safety research and development programs and for recommending any changes needed to protect the health and safety of the public. The AEC may still require information from licensees sufficient to provide an adequate basis for making judgments in particular cases, however, licensees should not consider such requests as a prejudgment of the issues.

One of the potential problems that might be encountered in implementing this criterion for backfitting would be a disagreement between the regulatory staff and the licensee as to the safety requirements agreed upon at the construction permit stage. The proposed amendment to the Commission's regulations will minimize this problem by providing for development and use during reactor construction of a system similar to the technical specification system presently being used during reactor operation. This new system will require delineation of the essential elements of the design and specify that these cannot be changed after issuance of the permit without prior Commission approval. Other design aspects can be changed at the licensee's discretion, subject to later review by the Commission at the operating license stage.

The Study Group believes that development and use of a system such as that outlined above would contribute to the stability of the licensing process.

H. The Role of the ACRS in the Regulatory Process

The Internal Study Group examined the role of the ACRS in the regulatory process with regard to the review of individual applications and the resolution of broader safety issues.

CONCLUSIONS AND RECOMMENDATIONS

1. The ACRS constitutes a valuable resource of the AEC. For optimum use of the Committee, its role in the regulatory process should be modified.
2. The ACRS should be relieved of the obligation to review and report on all applications for power reactor construction permits and operating licenses. The Committee should then gradually reduce its involvement in the reviews of individual applications and concentrate more on:
   (a) Safety issues involving a class of reactors, new concepts of reactor design and new approaches to accident prevention or consequence limiting safety features.
   (b) Evaluation of new data resulting from safety research and development programs and information gained during the construction and operation of power reactors.

(c) Development of regulatory criteria and standards relating to safety and the technical bases used in the regulatory review of individual applications.

DISCUSSION

The Atomic Energy Act presently requires the ACRS to advise the Commission as to the safety of each power reactor prior to the issuance of a construction permit and again prior to issuance of an operating license. This case by case review by the part-time advisory committee has produced valuable results.

In the Group's view, however, the relative utility of the present type of ACRS review must be viewed in the context of changing circumstances. As the number of similar plants and the relevant safety-related areas repeatedly reviewed have increased, the premises underlying regulatory approval of individual applications have been used increasingly to form the bases for regulatory criteria and standards. Although much remains to be done with respect to criteria and standards, significant progress has been made. With this background, and with the present depth and breadth of technical competence within the regulatory staff, the Study Group believes the staff is in a position to and should perform more of the case reviews alone, without an ACRS review. The consideration of the large volume of details inherent in an in-depth review of a particular application is best accomplished by a full-time, competent, professional regulatory staff.

In difficult cases, in cases where novel design approaches are proposed, and in cases for which regulatory criteria are not available, specific case reviews should continue to be made by the ACRS. But apart from those cases, the Study Group believes that it is in such areas as development of criteria and consideration of special safety issues, that a part-time expert committee can be most effectively and efficiently used.

It is the Group's view that the ACRS might better concentrate its efforts on safety issues involving a new class of reactors, new concepts of reactor design and new approaches to accident prevention or consequence limiting safety features. The Committee should also be in a position to evaluate new data resulting from safety research and development programs and information generated during the construction and operation of power reactors. And, of progressively increasing importance, the Committee should have sufficient time to make the maximum contribution to the development of regulatory criteria and standards relating to safety and the description of the technical bases used in the regulatory review of individual applications.

A change of this magnitude should not be undertaken abruptly. The Study Group believes that if the required enabling legislation is passed the ACRS should gradually reduce its involvement in individual applications and correspondingly concentrate its involvement on issues which affect overall safety and the criteria and bases on which the regulatory staff's safety reviews are made.

I. Timing and Staging in the Review and Decision-Making Process

A closer correlation is desirable between the timing of industrial decisions underlying the planning and execution of nuclear power plant projects and the timing of related decisions in the regulatory review process. This is particularly true with respect to the timing of decisions on siting and proposed plant design.

RECOMMENDATION

The Commission should explore the possibilities for revising the present regulatory review process with a view toward achieving one or more of the following objectives:

A. An earlier regulatory determination than at present on the matter of site suitability.

B. A phasing of regulatory design and construction approvals to correspond as closely as possible to the normal industrial plant design and construction phases.

C. An earlier construction permit decision than at present for reactors of established technology and generally standardized design, based on less documented design information in the application specific to the particular facility than is now required.

DISCUSSION

The industrial process of planning and achieving the production of power from a nuclear generating station involves a number of decision points. These include the decision to build a nuclear plant; the choice of a site; the selection of plant size, type and suppliers; the determination of the type of contracts and their execution; and the scheduling of construction so as to meet expected power needs.

The system for regulatory review of and decisions on power reactor license applications should provide the following:

1. A sound technical review of the reactor site, design, construction and operation proposed by the applicant.
2. Safety criteria, standards and codes, or other bases, upon which well-founded and timely regulatory decisions can be made.
3. A procedure which defines the scope and timing of regulatory reviews - relatively inflexibly and predictably for reactors of established technology.
4. The means for public scrutiny of regulatory reviews and the timely opportunity for those whose interests might be affected to have their views considered.

A lack of reasonable correlation between the timing of the decision points in the industrial process and the decision points in the system for regulatory review can have undesirable effects.

It may result in disc ntinuity in construction planning and extra costs for facilities; and, on a broader scale, it can be a possible hindrance to achieving the goal of economic nuclear power. Accordingly, an important area of consideration by the Study Group, to which much thought was given, was whether the decision points in the regulatory process could be better matched than at present with those in the industrial process.

Because the licensing process entails a review function, the timing of its decision points cannot correspond completely with the timing of industrial decision points. Industry representatives were of the view, however, that an improved correlation between the respective decision points can and should be made. In this regard, suggestions were received that the construction permit decision be made earlier and that there be greater predictability as to what will be approved. This would be done primarily by stabilizing the safety requirements underlying issuance of a construction permit (a matter discussed in other sections of this report), by limiting the scope of review at the construction permit stage or by a combination of the two. On a separate but related matter, the desirability of earlier opportunity for public participation in the regulatory review process - particularly with respect to the site - was also considered.

The Group believes that possible changes in the directions outlined above merit further serious consideration. In that connection, achievement of one or more of the following objectives appears desirable to the Group: (a) an earlier regulatory determination than at present on the matter of site suitability; (b) a phasing of regulatory design and construction approvals to correspond as closely as possible to the normal industrial plant design and construction phases; and (c) an earlier construction permit decision than at present for reactors of established technology and generally standardized design, based on less documented design information in the application specific to the particular facility than is now required.

The Group is not recommending any one particular course for achieving these objectives since any such restructuring of the regulatory review process should be preceded by a detailed exploration of relevant administrative, legal and other considerations. The Commission, however, may find it useful to consider three variations to the present review process which were discussed by the Study Group as means for furthering the stated objectives. These variations are described in outline below.

A. From the standpoint of the public and the utility, a regulatory review of site suitability would be preferable before any large commitment has been made by the utility and before there have been any irrevocable changes to the landscape. Since the suitability of a reactor site cannot be judged completely independently of the nuclear plants proposed to be located thereon, it would appear desirable that the Commission consider whether adequate criteria can be developed for siting reactors of established technology.

With such criteria, a mandatory public hearing on site suitability for reactors of that type could be held very early. Site preparation and initial foundation work would commence after this early hearing, to the extent such preconstruction permit work is now allowed under Part 50. A more detailed review of the proposed nuclear plant's design features would take place at a later time leading to the granting of a construction permit. Notice of proposed issuance of the construction permit would be given and a hearing would be held before an Atomic Safety and Licensing Board if any party, including a member of the public whose interest might be affected, requested such a hearing. Alternatively, notice of proposed issuance and an opportunity for a hearing might be dispensed with in view of the prior site hearing. There also would be a notice of proposed issuance and an offer of a public hearing prior to the granting of an operating license.

The principal resulting improvement in the regulatory process would be the earlier consideration of site suitability. A public review at that time could be valuable to the utility in providing early identification of potential site-related problems. It could also benefit those whose interests might be affected, such as local residents or representatives of interested States, by affording them an earlier opportunity to have their views considered on the safety questions involved. However, it is not clear to the Group, based on its limited study, what the problems might be in developing criteria suitable for this approach.

B. A possible variation to the changes in the regulatory process outlined in A., above, also appears to warrant further consideration for reactors of established technology. Under this variation, steps similar to those described in the preceding paragraph would be followed until the completion of the mandatory public hearing on site suitability. This hearing would be followed by a regulatory review of the design of the reactor plant; however, approval of construction would be in several stages rather than one stage. The several regulatory review stages would correspond as closely as possible to the actual industrial plant design and construction stages. There would not be an offer of a public hearing on these separate regulatory construction approvals, but there would be a notice of proposed issuance and an offer of a public hearing prior to the granting of an operating license. To be feasible, this approach would require development and approval of acceptable design interface conditions at the time of approval of any portion of the reactor plant design in order to assure compatibility of the several parts from a safety standpoint.

In addition to the potential advantages of earlier consideration of site suitability, discussed previously, this review approach would bring the regulatory decision points on construction authorization closer to the corresponding industrial decision points. At the same time, however, the increased number of decision points would place special emphasis on the need for making the regulatory decisions more predictable. This could be accomplished if adequate regulatory criteria can be developed concerning the design interface conditions previously referred to.

C. The correspondence between the regulatory and industrial decision points could be improved if the construction permit decision on acceptability of both the site <u>and</u> plant design could be made earlier in the review process than at present for reactors of established technology. This might be done by requiring less documented design information in the application specific to the particular facility than is the case under present procedures. A reduction in such documented information would, however, need to be compensated for by a corresponding increase in design standardization.

Under this approach, a construction permit review for a reactor of established technology might be limited, for example, to the proposed site, general reactor characteristics, and engineered safety features. Mandatory hearings at the construction permit stage might or might not be retained; but there would, in any event, be an opportunity for hearing at both the construction permit and operating license stages.

An earlier licensing decision on site and design matters could reduce the difficulties inherent in imposing regulatory requirements at a point in time after industry decisions and commitments have been made. However, to be fully useful, such a construction permit approval would have to be grounded on regulatory criteria, or other bases, sufficiently definitive to give reasonable assurance of issuance of an operating license upon satisfactory completion of facility construction.

The feasibility of this approach would seem to depend on the possibilities for stabilization of the scope of the construction permit review. For reasons discussed elsewhere in this report, these safety reviews presently require a substantial amount of information specific to the particular proposed reactor. However, the present trend toward standardization of design in water-cooled reactors, the movement in the direction of establishing more comprehensive safety criteria, codes and standards, and the research information and operating experience which will become available for the larger water-cooled reactors, may provide the basis for increased stabilization. It is in this context that the possibility for an earlier construction permit decision might be considered.

An additional observation is in order concerning each of the above approaches, or others which might be considered for the restructuring of decisional points in the review process. The public hearing phase of the safety review process has a bearing on the timing of regulatory decisions. Among those who spoke to the Group, opinion was divided as to the need for or desirability of a mandatory hearing at the construction permit stage - although all agreed that there should, as a minimum, be an opportunity for a hearing. A hearing on an uncontested construction permit application does involve some delay in issuance of a construction permit (approximately six to eight weeks, under current procedures), and there is a question as to whether the safety benefit derived from the limited board review warrants the time delay. However, from the standpoint of public participation and understanding, the hearing does appear useful and the delay could be mitigated if the hearing were held earlier in the development of the plant, as previously discussed.

One further matter warrants comment in connection with the subject of hearings. It was suggested to the Study Group that the role of the hearing board in an uncontested case might call for enlargement if there were a change in the present statutory requirement for ACRS review of each construction permit application. The Study Group does not agree with this view. The lack of need for an ACRS review - premised, presumably, on the absence of substantial or novel safety questions and confidence in the competence of the regulatory staff - should not be grounds for expanding the review function of the board. In this connection, it was recognized by all who commented to the Study Group that hearing boards, by virtue of their ad hoc composition, their discontinuous service and the constraints imposed by the limited periods for which they sit, are not in a position to carry out a comprehensive technical review of individual reactor applications. These circumstances further support the Group's view that the role of the boards should not be enlarged.

(15)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

Exhibit 1035

March 13, 1975

Commissioner Gilinsky

Thru: Acting Executive Director for Operations

TECHNICAL ISSUES

Attached you will find, in accordance with your oral request, discussion of some technical issues I believe to be important subjects for Commission consideration, although not necessarily in the immediate future. The list is confined to reactor safety topics.

I have also appended a list of some reactor safety policy issues that have come to my attention in technical reviews.

These enclosures represent my personal views and have not been staffed out with the organizations normally concerned with such matters.

Stephen H. Hanauer
Technical Advisor

Encls
1. Technical Issues
2. Policy Issues

cc: w/encl
Chairman Anders
Commissioner Kennedy
Commissioner Mason
Commissioner Rowden
L.V. Gossick
E. Case
H. Kouts
F. Schroeder
A. Giambusso
R. Minogue

AMERICAN REVOLUTION BICENTENNIAL 1776-1976

(48)

IMPORTANT TECHNICAL REACTOR SAFETY ISSUES FACING THE COMMISSION NOW OR IN THE NEAR FUTURE

1. Design Objectives and Safety Design Basis for Water Reactors

Although your mother-in-law and your Congressman will tell you that the safety goal is zero risk, we know that this is unattainable-and that some non-zero risk must be accepted in all activities. The social question involving cost/risk/benefit comparisons of the various alternatives that are realistically available needs to be established. The Rasmussen Study made an important first step in quantitative risk evaluation but the technology is not yet available to resolve this question in a completely quantitative way. The study has pointed out a disparity between (a) our present "design basis" safety approach in which all potential accidents are either put into the design basis for complete mitigation or remain outside the design basis and have no safeguards compared to (b) the more realistic viewpoint of a spectrum of accidents each with probability and consequences of its own. Serious consideration should be given to modifying the present all-or-nothing approach in the light of reality.

2. Design Objectives and Safety Design Basis for Non-Water Reactors

For non-water reactors, we have neither the operating experience nor the Safety Study to guide us in developing criteria. The situation is reasonably well in hand for HTGRs, but the potential for autocatalytic positive feedback leading to core nuclear explosions in LMFBRs is creating great uncertainty regarding their design requirements. Calculations of such violent events are increasing in scope and sophistication. However, the results presently depend to a considerable extent on the phenomena postulated to occur. For the near term, the staff has already decided that a core disassembly accident must be part of the licensing design basis. This decision is subject to future revision based on further research that ERDA is convinced will show that such events are so improbable they need not be considered.

Adequate safety must be provided. Too much safety - added safety equipment not actually needed to provide adequate safety - wastes scarce and valuable resources. Attention to improbable severe postulated events tends to short-change more probable but less severe accidents that should be considered.

An important corollary issue is whether the planned LMFBR safety research programs meet the totality of NRC needs.

3. Reliability and the Single Failure Criteria

NRC has not established quantitative reliability criteria for safety-related systems. The operating plants are one of our chief sources of information but we do not know whether the rate of abnormal occurrences now being experienced is a satisfactory one or not. We do know that nuclear unit availabilities and capacities are not satisfactory. We need to find out whether safety system availability is satisfactory and to improve whatever aspects of reliability need improving.

4. Human Performance

Present designs do not make adequate provision for the limitations of people. Means must be found to improve the performance of the people on whom we depend and to improve the design of equipment so that it is less independent on human performance.

The potential for internal and external sabotage constituting a public safety hazard, and the degree to which design and operation needs to take sabotage into account, need to be delineated. Studies now underway should help, but some of the issues are non-technical. In spite of this difficulty, technical criteria are needed.

The relative roles of human operation and automation (both with and without on-line computers) should be clarified. Criteria are needed regarding allowable computerized safety-related functions and computer hardware and software requirements for safety-related applications.

5. Plutonium Dose Criteria

Present accident dose guidelines values are given only for whole-body and thyroid doses. Other dose components (lung, GI tract, bone) should be covered by similar guidelines. A number (or numbers) for plutonium is particularly badly needed and will be particularly hard to establish.

6. Siting

Present criteria for siting are in need of improvement in the following areas:

a. The design basis external events now in use for licensing are founded on various schemes for estimating a "probable maximum" event. We do not have any good way of estimating the return interval or the frequency of the earthquake or flood calculated in this way. Furthermore we are not likely to develop good methods for doing so in the near future because of the short history (a few hundred years at best) and the long recurrence interval desired (sometimes we talk about a million years). Various developmental methods for estimating frequencies of design basis events, chosen as we choose them, give recurrence intervals substantially shorter than a million years. The lack of knowledge and the desire to be conservative is going to make resolution of this problem very difficult.

b. Our population siting criteria are indefinite at best. The applicant is required to study population distributions around a site and to project them for the life of the plant which, of course, he can do only very crudely, but our criterion for population distribution surrounding the plant are very vague. Recent attempts to be more quantitative in this area met with great resistance from the industry and from the old AEC. They tend to be oversimplified, but I believe we could do better than has been done. A related problem is our present total lack of control over what goes in near the plant after the site is approved. We have some vague words about the licensee's responsibility to stay informed about subdivisions, ammunition plants, LNG terminals and other post construction materialization of things that would have made the site unacceptable if known before licensing. Someday some operating reactor is going to have a new neighbor of a really abominable kind and we are going to have trouble coping with it.

c. I believe we are not being serious enough about siting alternatives that may offer substantial safety improvements. An obvious example is underground siting about which we are just starting a study in RES.

7. Degree of Detail and Realism in Safety Evaluations

The great improvement in computer codes available for use in analyzing the course and consequences of postulated accidents has rather naturally led to a corresponding increase in the depth and detail of Regulatory review of these accidents. On the face of it this is a good thing. It leads to better technical understanding and increased realism in evaluations. But is overall safety review enhanced by such detailed examination of certain design basis accidents? It is at least arguable that a broad brush treatment, with plenty of arbitrary conservatisms, gives at least as much safety with a lot less work on everybody's part. A recent and obvious example is the new ECCS regulation, which specifies in gory detail exactly how these calculations are to be made. There are many arguments for and against use of such details and the subject is about right for reopening, in my opinion.

A related subject is the very large increase in the capability of the NRC staff to make independent calculations in many accident areas. This has proved to be invaluable in increasing the staff's technical understanding and should be continued even if some of the details are recognized as too detailed for licensing.

8. Fuel Performance

The performance of light water reactor fuel in normal service has been disappointing to say the least. One would have thought that by this time fuel technology would be well developed. The appearance of such difficulties as densification, hydriding, hot pellets, and the recent incident at Dresden where a transient, well within all limits, resulted in unexpected fuel failures - all tell us that fuel technology is not in as good a state as we thought. The related technology of establishing fuel damage limits under accident conditions is even less well established, principally because PBF is so many years late.

9. Pu Recycle

This is not primarily a reactor problem. The reactor aspects seem to me to be adequately in hand.

REACTOR SAFETY POLICY ISSUES

1. Internal Quality Assurance

We are not taking our own medicine with regard to a quality assurance program in Reg. We do not have a quality assurance organization, independent of the line, reporting to higher management and we have very little auditing and QA in the line. If 10 CFR 50, Appendix B, is good stuff, then it should be applied to the NRC organization. This must be applied to the quality of our product - safety decisions - as well as the quantity and timeliness of our output.

2. Making Better, Faster and More Generic Decisions

Our recent record is mixed. A good example is ATWS and a bad example is turbine missiles, about which we seem not to be able to make up our minds. Future technical safety review should not be endless and mindless repetition of what we have been doing for the past couple of years but rather consolidation into general decisions and general principles, better identification of what is truly important (risk evaluation?), and increasing automation of routine evaluations.

3. Stabilization of Regulation Requirements and Standardization of Designs

Our recent reviews of the standardized designs that have been submitted and recent discussions on standardization (and piggy-back) show the following:

a. The standardization designs submitted are not consolidations of previous experience. The proposed standard designs include a large number of "improvements" not yet actually designed. So, these first standard CPs will be based on a bunch of promises, even more than recent custom CPs.

b. New information from design and operating experience and safety research programs, and new insights as a result of this experience and research have pointed the way to improvements in safety that seem worthwhile and in some cases necessary. The pace and guidelines of the standard reviews has not permitted implementation of these, so they are hanging over our heads as a serious threat to standardization.

c. As a result of a. and b. and of the long time lag between today's bunch of promises and construction and operation of standard plants, more attention needs to be paid to the execution of standardization over the next several years and stabilization of Reg requirements.

4. Too Many Surprises

This is closely related to Item 3. In the past couple of years surprises have come both from operating experience and from improved understanding by both Reg and the industry of safety problems we thought were put to bed. An obvious example is all the trouble we had with ECCS evaluation models. Innovation by applicants will continue to generate surprises. We must develop methods for dealing with these surprises, in cases and generically, without having a fire drill each time.

August 17, 1977

NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

Parler 417

SECY-77-439

INFORMATION REPORT

1036

E

FOR: The Commissioners

THRU: Lee V. Gossick, Executive Director for Operations

FROM: Edson G. Case, Acting Director, Office of Nuclear Reactor Regulation

SUBJECT: Single Failure Criterion

PURPOSE: To inform the Commission of the present status and future use of the Single Failure Criterion as a tool in the reactor safety review process.

DISCUSSION: A memorandum from the Secretariat to the Executive Director for Operations of June 30, 1977 requested that the staff maintain its schedule to develop an information paper on the Single Failure Criterion and its application. The enclosure provides that information.

The central conclusion to be drawn from this staff work is that the Single Failure Criterion has served well in its use as a licensing review tool to assure reliable systems as one element of the defense in depth approach to reactor safety. The Reactor Safety Study indicates that its use had led to a generally acceptable level of hardware redundancy in most systems important to safety. Some problems exist in specific interpretations and applications of the Single Failure Criterion, and these are the subject of ongoing work.

As for the future, the work underway will serve to codify and make more consistent our application of the Criterion in the licensing review process. It is expected that probabilistic methods of the type used in the Reactor Safety Study will gradually come into increasing use and supplement the Single Failure Criterion.

Edson G. Case, Acting Director
Office of Nuclear Reactor Regulation

Enclosure:
Information Paper on
Single Failure Criterion

DISTRIBUTION
Commissioners
Commission Staff Offices
Exec Dir for Operations
ACRS
Secretariat

Contact:
R. Ireland, NRR
49-28084

INFORMATION REPORT

BY THE

OFFICE OF NUCLEAR REACTOR REGULATION

ON THE

SINGLE FAILURE CRITERION

1. INTRODUCTION

The Single Failure Criterion is just one of several tools applied in systems design and analysis to promote reliability of the systems which are needed in a nuclear power plant for safe shutdown and cooling, and for mitigation of the consequences of postulated accidents. It is not sufficient by itself. Rules of good design practice, such as those required by the ASME Boiler and Pressure Code, IEEE standards, quality assurance requirements and conservatively stipulated design conditions must also be utilized to ensure that high quality and highly reliable systems, components and structures are provided.

The Single Failure Criterion, as a design and analysis tool, has the direct objective of promoting reliability through the enforced provision of redundancy in those systems which must perform a safety-related function. Simply stated, application of the Single Failure Criterion requires that a system which is designed to perform a defined safety function must be capable of meeting its objectives assuming the failure of any major component within the system or in an associated system which supports its operation.

The Single Failure Criterion was developed without the benefit of numerical assessments on the probabilities of component or system failure. However, in applying the Criterion, it is not assumed that any conceivable failure could occur. For example, reactor vessels or certain types of structural elements within systems, when combined with other unlikely events, are not assumed to fail because the probabilities of the resulting scenarios of events are deemed to be sufficiently small that they need not be considered. In general only those systems or components which are judged to have a credible chance of failure are assumed to fail when the Single Failure Criterion is applied. Such failures would include, for example, the failure of a valve to open or close on demand, the failure of an emergency diesel generator to start or the failure of an instrument channel to function. A single failure can also be a short circuit in an electrical bus that results in the failure of several electrically operated components to function.

The Single Failure Criterion, through enforced provision of redundancy, does not give absolute assurance of reliability. The Reactor Safety Study (WASH-1400) indicates that application of the Single Failure Criterion to the plants that were studied did provide an acceptable degree of hardware redundancy for most systems. However, the Reactor Safety Study also pointed out that factors such as systems interactions, multiple human errors, and maintenance and testing requirements also have an influence on reliability. Such factors fall outside the scope of the Single Failure Criterion, and supplementary methods must be utilized in their study.

At the present time, the Single Failure Criterion is codified in Appendix A to 10 CFR 50 (General Design Criteria) and in Appendix K (ECCS Evaluation Models); in addition, 10 CFR 50.55a (Codes and Standards) makes mandatory the use of the ASME Code and of IEEE Std 279 which contains the Single Failure Criterion. Further interpretation and guidance on the application of the Single Failure Criterion is given in the Standard Review Plan and Regulatory Guides (e.g., Standard Review Plan Section 3.6.1 describe its application in the event of postulated piping failures outside containment, and Regulatory Guide 1.53 endorses IEEE Std 379 which describes in detail how the Single Failure Criterion defined in IEEE Std 279 is applied to electrical and instrumentation systems).

2. IMPORTANT ELEMENTS OF THE SINGLE FAILURE CRITERION

A. The Concept

In principle, the Single Failure Criterion is straightforward. Simply stated it is a requirement that a system which is designed to carry out a defined safety function (e.g., an Emergency Core Cooling System) must be capable of carrying out its mission in spite of the failure of any single component within the system or in an associated system which supports its operation. Application of the concept is complicated by the interrelationships between the various fluid and electrical systems and their supporting auxiliaries in a nuclear power plant. Furthermore, there is a need to stipulate the events and associated assumptions which must be considered during application of the Single Failure Criterion.

Application of the Single Failure Criterion involves a systematic search for potential single failure points and their effects on prescribed missions (i.e., Failure Modes and Effects Analysis). Such a search is required by our Standard Review Plan and the Standard Format for the Content of Safety Analysis Reports for specified safety systems and components. The objective is to search for design weaknesses which could be overcome by increased redundancy, use of alternate systems or use of alternate procedures.

B. Definition of Single Failure

Single failure is defined in 10 CFR 50 Appendix A As follows:

> "A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of capability of the system to perform its safety functions."

A footnote to this definition states that "single failures of passive components in electric systems should be assumed in designing against a single failure." This means that for electric systems no distinction is made between failures of active and passive components and all such failures must be considered in applying the Single Failure Criterion. For example, short circuits in electrical cables must be considered even though a short circuit could be regarded as a failure of a passive component.

With regard to passive components in fluid systems, the footnote further states, "The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development."

While considerable progress has been made in defining the nature of passive component failures which should be considered in the licensing review process, no change to the regulation has been made since 1969. In application of the Single Failure Criterion to fluid systems, Section 6.3 of the Standard Review Plan requires consideration of passive failures in the Emergency Core Cooling System during the recirculation cooling mode following emergency coolant injection, but does not define the nature of such failures. Other interpretations of the Criterion for passive components have been made on the basis of detailed engineering evaluations conducted during licensing reviews, but with some staff disagreement. For example, NUREG-0138 (Issue 7) has a detailed discussion of passive failures following a Loss of Coolant Accident, and NUREG-0153 (Issue 17) has a detailed discussion of passive type valve failures. This subject is also summarized in Section 4 below and the status of standards development pertinent to this subject is summarized in Section 6. The following definitions of single active and passive failures in fluid systems important to safety are pertinent to the discussion of the Single Failure Criterion.

C. Active Failure in a Fluid System

An active failure in a fluid system means (1) the failure of a component which relies on mechanical movement for its operation to complete its intended function on demand, or (2) an unintended movement of the component. Examples include the failure of a motor- or air-operated valve to move or to assume its correct position on demand, spurious opening or closing of a motor- or air-operated valve, or the failure of a pump to start or to stop on demand. In some instances such failures can be induced by operator error.

D. Passive Failure in a Fluid System

A passive failure in a fluid system means a breach in the fluid pressure boundary or a mechanical failure which adversely affects a flow path. Examples include the failure of a simple check valve to move to its correct position when required, the leakage of fluid from failed components, such as pipes and valves--particularly through a failed seal at a valve or pump--or line blockage. Motor-operated valves which have the source of power locked out are allowed to be treated as passive components.

In the study of passive failures it is current practice to assume fluid leakage owing to gross failure of a pump or valve seal during the long-term cooling mode following a LOCA (24 hours or greater after the event) but not pipe breaks. No other passive failures are required to be assumed because it is judged that compounding of probabilities associated with other types of passive failures, following the pipe break associated with a LOCA, results in probabilities sufficiently small that they can be reasonably discounted without substantially affecting overall systems reliability.

It should be noted that components important to safety are designed to withstand hazardous events such as earthquakes. Nevertheless, in keeping with the defense in depth approach, the staff does consider the effects of certain passive failures (e.g., check valve failure, medium or high energy pipe failure, valve stem or bonnet failure) as potential accident initiating events.

3. APPLICATION OF THE SINGLE FAILURE CRITERION

As noted previously, the events and associated assumptions which are considered in connection with application of the Single Failure Criterion must be defined for specific systems. The basic events and assumptions are defined in the General Design Criteria.

A variety of design basis events which initiate a requirement for safety system action must be considered in the overall safety evaluation of a plant. In general, each of these initiating events requires an assessment of the equipment damage that could occur as a direct consequence of the event. The Single Failure Criterion is applied to those systems which must function after consequential equipment failures have been taken into account.

The General Design Criteria make it clear that for electrical, instrumentation and control systems, application of the Single Failure Criterion to systems evaluation depends not only on the initiating event that invokes safety action of these systems, together with consequential failures, but also on active or passive electrical failures which can occur independent of the event. Thus, evaluation proceeds on the proposition that single failures can occur at any time.

In contrast, for various fluid systems the General Design Criteria require that the safety function be accomplished in the face of certain conservative assumptions in addition to application of the Single Failure Criterion. In general, these assumptions involve (1) the unavailability of offsite or onsite power and (2) the postulated initiating failure. In the case of a loss of coolant accident, for example, it is first assumed that a primary system pipe rupture occurs with consequential blowdown of primary coolant.

Simultaneous with the pipe rupture, it is assumed that only the offsite power source or the onsite emergency power source is available.(1) These assumptions are applied in addition to the Single Failure Criterion which is applied to the aggregate of systems required to fulfill each specific safety function.

The manner in which the Single Failure Criterion is currently applied to various specific classes of safety related systems is outlined below.

A. Electrical, Instrumentation and Control Systems

The general interpretation and application of the Single Failure Criterion to electrical, instrumentation and control systems is stated in IEEE Std 379 as follows:

> "The system shall be capable of performing the protective actions required to accomplish a protective function in the presence of any single detectable failure within the system [this is the "single failure"] concurrent with all identifiable, but non-detectable failures, all failures occurring as a result of the single failure, and all failures which would be caused by the design basis event requiring the protective function."

---

(1) Successful emergency systems performance must be demonstrated with either offsite or onsite power, assuming a single failure.

Therefore, in the analysis to determine if a particular electrical, instrumentation or control system meets the Single Failure Criterion the following postulates are made:

(1) First, the particular design basis event or accident is postulated to occur, along with any related or consequential failures that could result from it.

(2) Then, the analysis assumes the presence of all identifiable failures which cannot be detected or tested in the design or which are not in fact subject to surveillance tests as set forth in the Technical Specifications.

(3) Finally, the presence of a single additional detectable failure is assumed in assessing the capability of the system to provide the necessary protection for the design basis event.

Analyses are performed in this manner to demonstrate the adequacy of the electrical, instrumentation and control systems design over the full range of postulated design basis events or accidents and worst case single failures.

There is a special interpretation of the Criterion (Section 4.7 of IEEE Std 279) which specifically addresses designs in which safety-related instrumentation or controls are also used to provide inputs to non-safety related plant control systems. In such a design it is required that where a single random failure in the safety-related system can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure. This special interpretation of the Single Failure Criterion is specific for the design cited above, and it is not applied to safety-related electric power systems.

The general interpretation of the Single Failure Criterion is applicable to safety-related electric power systems. However, the offsite power system is an exception. The specific requirements of General Design Criterion 17 take precedence over the rigorous application of the Single Failure Criterion; i.e., an offsite power system comprised of one delayed access circuit and one immediate access circuit is deemed acceptable. The basis for this position is that a second immediate access circuit would not significantly improve the availability of offsite power at the emergency buses. This has been established by an analysis using reliability data and not the Single Failure Criterion.

B. Emergency Core Cooling Systems

In applying the Single Failure Criterion to Emergency Core Cooling Systems which must function following postulated loss of coolant accidents, the requirements of General Design Criterion 35 - Emergency Core Cooling - are followed. Therein it is stipulated that following a postulated loss of coolant accident, suitable redundancy in equipment shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the ECCS safety function can be accomplished, assuming the most limiting additional single failure. Appendix K to 10 CFR 50 requires that the only ECCS subsystems to be assumed available are those operable after the most damaging additional single failure of ECCS equipment has taken place. Selection of the single failure to be applied to the emergency core cooling system is made independent of the size or location of the postulated pipe break in the reactor coolant system. Thus, for each postulated pipe break, that single failure which results in minimum emergency core cooling performance is considered in judging the adequacy of the system. For example, this could be failure of a component in a redundant ECCS subsystem or the loss of an emergency diesel generator in addition to the loss of all offsite power.

During the short-term ECCS coolant injection mode immediately following a loss of coolant accident, the most limiting single active failure is considered in evaluating systems performance capability.

During the long-term ECCS recirculation cooling mode the most limiting active failure, or a single passive failure equal to the leakage that would occur from a valve or pump seal failure, is assumed. The basis for not including other passive failures during the long term is based on engineering judgment that such failures (pipe or valve breaks) have an acceptably low likelihood of occurrence during the long-term phase of a loss-of-coolant accident. Analyses of ECCS performance in WASH-1400 indicate that passive failures of valves and piping are relatively small contributors to ECCS unavailability during both the injection and recirculation modes of operation.

C. Containment Heat Removal and Cleanup Systems

General Design Criterion 38 - Containment Heat Removal - requires the provision of a system to rapidly reduce containment pressure and temperature following any LOCA. While current practice is to apply only an active component failure to the evaluation of the performance of these systems, component redundancy ensures their availability even in the presence of some possible passive failures.

General Design Criterion 41 - Containment Atmosphere Cleanup - requires systems to control fission products, hydrogen, oxygen, and other substances which may be released into containment. These systems must be capable of functioning with either onsite or offsite power. Contaminants can enter the containment due to a variety of events, such as a LOCA. The Single Failure Criterion is applied subsequent to the postulated event and, in evaluating these systems, only active failures are considered, except in instances where components may be shared with ECCS systems. In such cases, the possibility of seal leakage is considered in the long-term ECCS recirculation mode.

D. Residual Heat Removal System

The capability for residual heat removal must be available using onsite or offsite power, assuming an additional single failure. To accommodate certain single failures, for the older class of plants, the staff has accepted use of the auxiliary feedwater system as a backup to the residual heat removal system. For current designs, the residual heat removal system has been modified to include additional piping and valves such that the system now has additional flexibility to perform its function even after a wide range of possible single failures. Also, as part of current staff reviews, certain initiating events have been postulated which are related to the Single Failure Criterion. These events involve application of the pipe break criteria for moderate energy lines located outside of containment as described in Standard Review Plan 3.6.1. Thus, the staff applies a limited passive failure as an initiating event for the residual heat removal system. For this event, no additional single failure is applied to the Residual Heat Removal System.

E. Ultimate Heat Sink

General Design Criterion 44 - Cooling Water - requires a system to transfer heat from systems, structures, and components important to safety to an ultimate heat sink under normal operating and accident conditions. The system must be capable of carrying out its function using either onsite or offsite power assuming any single failure. The requirements of the Single Failure Criterion are applied in a manner similar to that which is applied to residual heat removal systems.

F. Containment Piping Penetrations

Requirements for isolation valves on containment penetrations are defined in the General Design Criteria. The requirements anticipate the possibility of single active failure of isolation valves in each line by requiring double barriers. The Single Failure Criterion is also applied to the plant protection devices which initiate automatic closure of such isolation devices.

4. PROBLEMS THAT HAVE BEEN ENCOUNTERED IN THE APPLICATION OF THE SINGLE FAILURE CRITERION

A. Additional Passive Failures

As stated previously, there is a footnote in the General Design Criteria that the conditions under which single passive failures should be considered in applying the Single Failure Criterion to fluid systems are under development. That footnote was included when the Criteria were published in 1969. During subsequent years staff assumptions regarding the nature of passive failures which should be considered have not been completely consistent and there has been some disagreement. However, on the basis of the licensing review experience accumulated in the period since 1969, it has been judged in most instances that the probability of most types of passive failures in fluid systems is sufficiently small that they need not be assumed in addition to the initiating failure in application of the Single Failure Criterion to assure safety of a nuclear power plant. This opinion appears to have been verified by the Reactor Safety Study. Nevertheless, it is receiving further study.

In some licensing review areas, the staff does impose a passive failure in addition to the initiating event, while in others it does not. As previously mentioned, an example of the application of a passive failure requirement is the approach to long-term recovery subsequent to a loss-of-coolant accident. Applicants are required to consider degradation of a pump or valve seal and resulting leakages in addition to the initiating failure (LOCA). The rationale for applying this type of failure is a recognition of the relatively extended periods of required operation of systems that are expected to be on a standby status throughout the plant life. The likelihood of accelerated wear of such components as pump and valve seals would be increased after the adverse conditions following a LOCA. Extended operation during the long term (up to months) requires that these types of failures be considered in designing the plant. The basis for excluding additional passive piping failures is elaborated in detail in NUREG-0138, Issue 7. Other examples of passive failure considerations are presented in Section 4.B.

B. Valve Failures

A variety of valve functions and valve types exist in each nuclear plant. Valve functions include isolating flow, controlling flow, admitting flow, and preventing flow reversal. Valve types include those that are electrically controlled and operated, electrically controlled and air operated, manually controlled and operated, manually controlled and electrically operated, spring operated, and self actuated (check valves).

Accordingly, a variety of failure modes can be postulated for valves within the application of the Single Failure Criterion. Certain passive-type valve failure modes have occurred (for example, dropping of a valve disc). This has resulted in a reevaluation of postulated valve failures. NUREG-0153 (Issue 17) concludes that while the staff does not consider that changes in safety criteria are warranted at this time, ongoing efforts regarding the probability and effects of various valve failure modes will seek to compile a more rigorous data base and will apply such information to plant safety analyses. This effort has been classed as a Category B generic task.

C. Electrical Failures

In order to provide an electrical, instrumentation and control system design to satisfy the Single Failure Criterion, redundancy is included. The degree of redundancy (i.e., the number of "independent" divisions of equipment) depends on many design considerations. Provisions are typically included to prevent the initiating event from affecting the electrical, instrumentation and control systems.

If it is postulated that the failure of a portion of the safety-related electrical, instrumentation and control systems is the initiator of a design basis event, then the general interpretation of the Single Failure Criterion, discussed in Section 3.A, is not applicable to the remaining portions of the system. In such cases supplementary analyses are relied upon to evaluate the reliability of the systems in question.

In the case of the current issue on the reliability of the safety-related direct current power systems as raised by an ACRS consultant, the postulated initiating event is failure of one division of a two division system. However, this DC power system design does meet the general interpretation of the Single Failure Criterion, but it is not covered by the special interpretation noted in Section 3.A for specific safety-related instrumentation and control systems. Therefore, the staff evaluation of this issue, summarized in NUREG-0305, was based upon reliability data and not the Single Failure Criterion. It was concluded that the likelihood of occurrence of the postulated sequence of events is low enough to permit continued operation and licensing of plants pending further assessments. It is possible that new requirements to assure greater reliability of DC power systems may result from the ongoing study. It is a Category A generic task.

D. Classification of Events

Recent staff work related to issues raised in dissent or pertaining to reactor transient event classifications and consequence criteria has disclosed some confusion on how to handle certain infrequent transients which do not have public consequences as severe as "accidents". The confusion stems primarily from the differences in event classification from vendor to vendor, among standards writing bodies and within NRC. A study is underway within the Reactor Systems Branch to develop a "unified" event classification scheme. It is expected to be completed in early 1978. While this study is not aimed at application of the Single Failure Criterion, it is expected that for some events it will bring into sharper definition the circumstances under which the Criterion should or should not be applied. For example, a moderate frequency transient such as a feedwater malfunction is routinely analyzed in Safety Analysis Reports. An additional single failure concurrent with the feedwater malfunction may result in a compound event which, because of the multiple failures, has a lower probability and therefore a different classification. Less stringent acceptance criteria may then be appropriate. The above study will examine such additional single failures as they apply to acceptance criteria for transients and accidents. This study has been classed as a Category B generic task.

E. Operator Error

An operator error could cause an active single failure, such as an inadvertent valve closure. In many instances consideration of such single operator errors is given in licensing reviews; however, the degree to which any given operator error is considered reasonably equivalent to the likelihood of a single active failure is based on judgments made concerning the situation. For example, in studying the effects of an operator error of "omission" (failure to perform an action), if there is time to bring a system on line through remedial operator action, reliance on such action is permitted. On the other hand, in cases where rapid actuation of engineered safety systems is required, the actuation is required to be automatic and operator independent.

Increasing attention is being given to human reliability in an effort to adopt more definitive criteria for the role of the operator in mitigating the consequences of transients or accidents. A Regulatory Guide is currently being developed in conjunction with staff review of the proposed Standard ANSI-N660, "Proposed ANS Criteria for Safety-Related Operator Actions." Increasing activities in human reliability will assist the staff in developing a more rigorous basis for assessing operator involvement in plant safety.

5. INSIGHTS OF THE REACTOR SAFETY STUDY RELATIVE TO THE SINGLE FAILURE CRITERION

The Reactor Safety Study (WASH-1400) assessed a pressurized water and a boiling water reactor design. The Single Failure Criterion had been applied in the design and Regulatory review processes for these plants, generally as outlined in the preceding sections. Although the Single Failure Criterion is not a quantitative design and analysis tool, the numerical assessments in the Reactor Safety Study indicate that its application, through enforced provision of component and systems redundancy, has made an important and necessary contribution to the overall reliability of nuclear plant safety systems. The assessments in the Reactor Safety Study also indicate that supplementary methods of analysis must be utilized to study effects on reliability which are beyond the scope of the Single Failure Criterion. The principal insights gained from this study are briefly summarized below:

(1) Application of the Single Failure Criterion has led to a suitable level of hardware redundancy in most systems. The level of redundancy thus provided has, for many safety systems, resulted in systems reliability being controlled by such factors as human and operational interactions (i.e., human errors, test and maintenance downtimes, test intervals) rather than potential single design failures as defined in the Single Failure Criterion.

Quantitative optimization of reliability in terms of such non-hardware factors would require the review of information beyond that now considered in the licensing process.

(2) The Single Failure Criterion must be supplemented by methods and criteria in the area of common mode assessments if improved reliability characteristics for safety systems are necessary. Although the effects of common mode failure are not now quantitatively considered in licensing safety reviews, considerable attention is given to reducing the potential for the occurrence of common mode failures through stringent application of high-quality design and quality assurance requirements to various components. For example, considerable attention is given to reducing the potential for multiple electrical relay failures such as might arise from a generic design defect in components supplied by a single manufacturer.

(3) The probability of accident sequences resulting in core meltdown were found by the RSS to be importantly influenced by system to system interactions and by functional dependencies between systems. These functional dependencies can be considered as a class of interactions where the functioning of one system depends on satisfactory functioning of another system. Redundancy of components within systems, mandated by the Single Failure Criterion, does not ameliorate the functional dependence. Thus, application of the Single Failure Criterion requires supplemental methods and use of an integrated systems approach to identify such functional dependencies if it is desired to further reduce accident risk.

6. ACTIVITIES RELATED TO CLARIFYING AND IMPROVING APPLICATION OF THE SINGLE FAILURE CRITERION

A number of technical activities by various nuclear industry groups and by the Offices of Standards Development and Nuclear Reactor Regulation are underway, which will have an effect on system reliability requirements and the use of the Single Failure Criterion. These are summarized in this section.

In late 1971 the American Nuclear Society initiated a standards writing effort with the objective of setting forth a clear, detailed set of criteria for application of the Single Failure Criterion to fluid systems. In 1975 the resulting Standard was issued as "ANSI N658 - Single Failure Criteria for PWR Fluid Systems." In November of 1976, the Office of Standards Development initiated a task to draft a Regulatory Guide endorsing the Standard, with appropriate exceptions, for both PWRs and BWRs. The staff review of this Standard disclosed several deficiencies which relate primarily to inconsistencies with current regulatory practice and to areas in which staff application of the Single Failure Criterion is not yet fully defined. For example: (1) literally applied to "postulated pipe breaks outside containment," the Standard would make no exception for certain dual purpose moderate energy systems (e.g., service water systems) as presently provided in Standard Review Plan 3.6.1; (2) some passive failures would be treated as active failures (e.g., check valves) contrary to staff practice; and, (3) event categorization is not consistent with current staff interpretation. Nevertheless, ANSI-N658 represents a significant step toward achieving satisfactory criteria for application of the Single Failure Criterion to fluid systems, and it is expected that a Regulatory Guide could be issued in mid-1978.

IEEE Std 379 was issued in 1972 as a Trial-Use Guide for the Application of the Single Failure Criterion to Electrical, Instrumentation and Control Systems and its application was endorsed in Regulatory Guide 1.53. IEEE Std 379 was recently updated and reissued. The subcommittee which prepared the Standard is currently working to develop definitive guidance on application of the Single Failure Criterion to shared systems and to single operator errors. When this work is completed it is expected that Regulatory Guide 1.53 will be revised to endorse these added requirements.

Earlier this year, the Office of Nuclear Reactor Regulation initiated a formal system providing for continuing management oversight and attention to generic safety-related technical activities. A number of these generic activities may include clarification of the conditions under which the Single Failure Criterion should be applied. The Category A activities expected to include single failure considerations are:

(1) Anticipated Transients Without Scram;

(2) Non-Safety Loads on Class IE Power Supplies;

(3) Adequacy of Safety-Related d.c. Power Supplies;

(4) Reactor Vessel Pressure Transient Protection;

(5) Steam Line Breaks;

(6) RHR Shutdown Requirements;

(7) Systems Interaction; ~~and~~

(8) Generic Accident Risk Study

(9) Snubbers

The Category B activities expected to include single failure considerations are:

(1) Event Categorization;

(2) ECCS Reliability;

(3) Locking Out of ECCS Power Operated Valves;

(4) Protection Against Postulated Piping Failures in Fluid Systems Outside Containment;

(5) Criteria for Safety-Related Operator Actions;

(6) Passive Mechanical Failures; and

(7) Allowable ECCS Equipment Outage Periods

In some cases these activities are being conducted to evaluate adequacy of previous staff positions, while in others some new provisions may result. The single failure aspects of these activities will be utilized as appropriate in connection with improving application of the Single Failure Criterion.

The NRR staff is developing a plan for incorporating risk assessment methodology into the licensing process. Because of manpower limitations, and the need to train an initial cadre in risk assessment methodology and to carefully weigh impacts of its application, it is expected that application of risk assessment methodology to the licensing process would necessarily increase gradually over a period of several years. It is not expected that risk assessment methodology will come into large-scale systematic use in the near future as a replacement for the Single Failure Criterion as it is now applied. It is expected, however, that reliability engineering and probabilistic methodologies, together with an expanding data base on component and systems failure rates, will be applied to specific studies pertaining to reliability requirements and evaluations that go beyond the Single Failure Criterion. The current study of the adequacy of DC power supplies is an example of such an application.

7. SUMMARY CONCLUSIONS

Application of the Single Failure Criterion as it is presently defined in the regulations, Standard Review Plan, and various Regulatory Guides and industry standards has led to a generally acceptable level of hardware redundancy in most electrical, control and instrumentation systems and in fluid systems important to safety. As indicated by the Reactor Safety Study, systems unavailabilities are controlled to a large extent by factors such as operator errors, systems interactions, and maintenance and testing requirements, rather than by inadequate hardware redundancy. Some problems exist in specific interpretations and applications of the Single Failure Criterion and these are receiving staff attention. It is the considered judgment of the staff that the Single Failure Criterion should continue to be applied subject to resolution of specific problem areas currently defined and under study, pending any long-term wide-scale incorporation of reliability and risk assessment methodology into the licensing process.

Exhibit 1037

Appendix C

GENERAL ADVISORY COMMITTEE
to the
U. S. Atomic Energy Commission
P. O. Box 3528
Washington 7, D. C.

April 3, 1961

Dr. Glenn T. Seaborg, Chairman
U. S. Atomic Energy Commission
Washington 25, D. C.

Dear Glenn:

The 73rd meeting of the General Advisory Committee was held in Washington, D. C. on March 22, 23, and 24, 1961. With the exception of Dr. Norman Ramsey who attended only the morning session on March 24, all other members were present during all sessions. These were Philip H. Abelson, Manson Benedict, W. F. Libby, Eger V. Murphree, J. C. Warner, Eugene P. Wigner, John H. Williams, and K. S. Pitzer, as Chairman. Also present were Robert A. Charpie, Secretary, and Anthony A. Tomei, Assistant Secretary.

The following recommendations and actions of the Committee are herewith presented:

(1) Safety Policy and Organization

The GAC devoted most of its time during this meeting to briefings and discussions on the AEC's safety policies and practices. We wish to record our appreciation of the efforts of the AEC staff in preparing and presenting these briefings.

The Committee devoted particular attention to the Commission's new organization scheme for licensing and regulatory activities. The Committee also met with the Chairman of the ACRS in order to understand the relationship of the ACRS to the Commission's staff activities associated with safety. On the basis of these discussions we believe that the AEC's regulatory activities are presently organized to attack all of the major areas which require such regulation. The most serious limitation arises from a shortage of well trained and able inspectors of technical operations. This personnel shortage will limit the effectiveness of inspection of the AEC's own operations in the near future.

The GAC will continue its review of the safety question in the future. At the present time we offer the following comments and recommendations:

(a) We recommend that AEC policy require an absolutely clear assignment of responsibility for the safety of each reactor, whether AEC owned or non-AEC owned. In this connection we recommend the establishment of the profession of Reactor Captain. The Reactor Captain should be in absolute charge of a facility, in the same sense as a ship's captain. We believe that the qualifications for a Reactor Captain should be established by the AEC. He should pass the Reactor Operators' examination, however, he must know much more than an Operator. Captains must demonstrate the thorough understanding of reactors which absolute responsibility entails. Finally, we do not believe the AEC must insist on having a Reactor Captain constantly on duty in every reactor since there are certain very low-powered reactors which are inherently much less hazardous than other types.

(b) We are concerned by Mr. Johnson's report on inhalation hazards in our Western uranium mines. We recognize that the AEC does not control the mines nor deal directly with the mine operators. Unfortunately the AEC cannot disavow its responsibilities no matter how indirect the administrative relation may be. We recommend that the AEC continue to work with the mine operators and the regulatory groups in the States to reduce the air contamination levels in the uranium mines to more satisfactory levels.

(c) We believe it would be desirable for the AEC to be better informed of reactor safety policies in other countries. It has always seemed logical to us that the IAEA is a natural organization for promoting the exchange of such information. It would seem to us to be appropriate for the U. S. to take the leadership in suggesting this role for IAEA. An important collateral benefit to the U.S. from such an activity would be to increase the possible psychological impact to be derived from the N. S. Savannah by making more ports available to it.

(d) While the scientific understanding of the SL-1 incident is still incomplete, the facts are sufficiently clear to provide a basis for decision concerning management inadequacies. The GAC trusts that the Commission action in this area will be prompt and decisive. The GAC will be interested to learn about these actions in the near future.

DELETED

Respectfully submitted,

/s/ Ken

K. S. Pitzer
Chairman

1030
Bx.

Parker

AMERICAN PHYSICAL SOCIETY

[illegible] GROUP ON LIGHT WATER REACTOR SAFETY

[illegible] 197[illegible]

[illegible] IN THE REVIEWS OF MODERN PHYSICS

REPORT TO THE AMERICAN PHYSICAL SOCIETY

BY THE

STUDY GROUP ON LIGHT-WATER REACTOR SAFETY

28 April 1975

H. W. Lewis (Chairman)	University of California, Santa Barbara
R. J. Budnitz	Lawrence Berkeley Laboratory
A. W. Castleman	Brookhaven National Laboratory
D. E. Dorfan	University of California, Santa Cruz
F. C. Finlayson	Aerospace Corporation
R. L. Garwin	International Business Machines Corporation
L. C. Hebel	Xerox Corporation
S. M. Keeny, Jr.	The MITRE Corporation
R. A. Muller	University of California, Berkeley
T. B. Taylor	International Research and Technology Corporation
G. F. Smoot	University of California, Berkeley
F. von Hippel	Princeton University

APS Council Review Committee:

Hans Bethe	Cornell University
W.K.H. Panofsky	Stanford Linear Accelerator Center
V. F. Weisskopf	Massachusetts Institute of Technology

Supported by the National Science Foundation and the Atomic Energy Commission. Contract EN-43893.

To be published in the Reviews of Modern Physics.

FOREWORD AND ACKNOWLEDGEMENTS

The American Physical Society has engaged over the past few years in activities beyond those traditional for the Society. In 1973 the Society explored mechanisms by which it could contribute to the alleviation of the energy crisis. In addition to other activities, it was decided to sponsor a study of reactor safety, an important subject with substantial scientific and technological content. This is the report of that year-long study by a dozen part-time participants with various levels of prior experience in the reactor field. The group met in Los Alamos during the month of August, 1974, and also had approximately a dozen two-day meetings, many phone calls, and much correspondence.

The group is grateful to all the genuine experts who gave liberally of their time in educating us about this intricate subject. In turn, we hope that our report will help inform the scientific and technical community about some of the technical issues of reactor safety.

We particularly acknowledge the contributions of S. Johnson, G. Brockett, and P. Davis, who served as consultants and who provided continuing support to our Study. Their patient exposition of the fine points of reactor design, operation and regulation was invaluable. We also particularly acknowledge the contributions of D. H. Coward, who helped organize the group, and of H. A. Bethe, W. K. H. Panofsky, and V. F. Weisskopf, who served as the APS Council Review Committee.

The cooperation of the reactor community and of experts in related fields such as biological effects of radiation was outstanding, and we acknowledge the help of the many representatives of the vendors, reactor

designers, safety analysts, and others who provided us with information. In particular, members of the staffs of the AEC* Division of Reactor Safety Research and of the AEC Directorate of Licensing gave willingly of their time and resources; the individuals involved are too numerous to mention by name. Also, the group is grateful for briefings and cooperation from all four American vendors of light-water reactors: Babcock & Wilcox, Combustion Engineering, General Electric, and Westinghouse. It is fair to say that we do not feel that we have been excluded from any information necessary to our task.**

We were fortunate that early in our study, we were given copies in preliminary draft of the AEC-sponsored study of reactor safety (chaired by Professor Norman Rasmussen of M.I.T., and known as WASH-1400). WASH-1400 is a detailed event-tree and fault-tree analysis of light-water reactor accident sequences. Its purpose was to make a quantitative estimate of the likelihood of accident consequences of a given severity. We did not undertake a review of that study as such, although it will be mentioned frequently in our report.

---

*Since this work was begun the Atomic Energy Commission has been split in two parts: the Energy Research and Development Administration (ERDA) and the Nuclear Regulatory Commission (NRC), and the exact distribution of the reponsibility that formerly resided in the AEC between ERDA and NRC is still not clear. For this reason we have referred throughout the report to the AEC with the understanding that the reader will interpret all forward-looking references to the AEC as really directed to the relevant components of ERDA or NRC.

**There is one exception. Early in our study we became interested in the safety record (in particular primary system integrity) of naval reactors, which, though smaller, have accumulated more reactor years of service than have the civilian reactors of comparable design. We made a major effort to obtain sufficient information, with due regard for questions of classification and national security, to help us in our study. We were refused any access by Admiral H.G. Rickover.

The gracious hospitality of the Los Alamos Scientific Laboratory and the administrative assistance of the staff of the American Physical Society are also acknowledged. This Study was supported by the National Science Foundation and the U.S. Atomic Energy Commission.

The study participants have all agreed on both the broad conclusions and the more detailed individual recommendations contained in the body of the report. We believe this is significant in view of the diverse backgrounds of the group. Our individual technical expertise ranges widely, covering theoretical and experimental physics, chemistry, and engineering. While a few of the group had some background in reactor safety, the majority of the group had not previously considered these issues. Some of the group had participated in previous technical assessments of broad national issues; for several others, this study was a first experience. We are pleased with the degree of consensus that we have achieved; albeit regretful that more time was not available for further investigation of some of the important issues involved.

I. SUMMARY OF CONCLUSIONS AND MAJOR RECOMMENDATIONS

A central issue in the operation of light-water reactors is the prevention of a major release and widespread dispersal of radioactivity, which could have serious consequences to the public. The safety record of light-water reactors to date has been excellent, in that there has been no major release of radioactivity. These reactors have been designed with numerous safety features, engineered to prevent foreseeable accidents. These safety features are backed up by other safety features intended to prevent major release of radioactivity in the event of an accident. Moreover, very conscientious efforts have been made in developing the procedures and practices involved in licensing, quality assurance, operation, and inspection of these reactors to insure sound construction and operation within specified safety limits.

In the course of this study, we have not uncovered reasons for substantial short-range concern regarding risk of accidents in light-water reactors. While at present a complete quantitative assessment of all important aspects of reactor safety and behavior under unusual circumstances cannot be made, we are confident that a much better quantitative evaluation and consequent improvements of the safety situation can be achieved over the next decade if certain aspects of the safety research program are substantially improved and the results of the research are implemented. Because of the serious potential consequences of a major release of radioactivity and in view of existing safety-related technological opportunities, we believe that there should be a continuing major effort to improve light water reactor safety as well as to understand and mitigate the consequences of possible accidents. Our recommendations are directed towards these objectives.

A. Safety through Careful Design, Construction, and Operation

The safety philosophy of the nuclear industry has emphasized design which can provide tolerance against malfunctions. This approach has laid a good foundation for reactor safety, and it has resulted in reactors designed, constructed, and operated for safety, not only under normal operating conditions but also in a wide range of abnormal circumstances. A great deal of research, development, and quality control has gone into guaranteeing the integrity of the fuel elements and cladding, the integrity of the enclosing primary system, the general structural soundness of the entire reactor, and the ability to control the reactor under both normal and abnormal conditions.

Although we have not been able to analyze all of the many possible failure sequences for light-water reactors, one which we have studied in detail is the possible failure of the integrity of the primary reactor pressure vessel. We find that reactor vessels are constructed of materials chosen with care and are designed with substantial safety factors. The reactor vessel is subject to careful scrutiny and testing. Based on our study, we believe that catastrophic rupture of the primary pressure vessel is not likely to be an important contributor to accident initiation; however, this is dependent upon maintaining a strong quality assurance program.

Primary system piping is also subject to careful scrutiny and testing. The well-known cases of cracks in pipes and failures of valves in reactor operation, on the one hand, reflect deficiencies in fabrication or design; but, on the other hand, they are a demonstration of the success of the overall safety system and procedures which identified their existence early enough to prevent more serious consequences. Continued open discussion and analysis of such failures can lead to improvements in safety and can provide the data base for a more accurate estimate of the probability of more serious incidents. These defects underline the on-going need for the nuclear industry and the regulatory bodies to continue improvement of inspection and test techniques. It is important that licensing and regulation be conducted in such a way as to continue to ensure openness in the quality assurance program and to provide better-quantified evaluation of the success of the program. We also note that human error on the part of reactor operators seems to initiate or aggravate at least a few incidents each year of potential safety significance. In fact, unless diligence is maintained, quality assurance and human error may well represent a limiting factor in maintaining safe operation.

It is difficult to quantify accurately the probability that any accident-initiating event might occur. Many aspects need to be better understood through experience and research before such calculations are tractable. Although the probabilities of major accidents seem small, their quantification deserves more attention within the reactor safety community than it has received up to now. We did not have the resources to carry out an independent evaluation of this aspect of the recent AEC Reactor Safety Study (draft WASH-1400), but we recognize that the event-tree and fault-tree approach can have merit in highlighting <u>relative</u> strengths and weaknesses of reactor systems, particularly through comparison of different sequences of reactor behavior. However, based on our experience with problems of this nature involving very low probabilities, we do not now have confidence in the presently calculated absolute values of the probabilities of the various branches.

We have reservations about the present almost exclusive emphasis in the licensing process on the 'design basis accident' concept in which certain highly stylized accidents are used as yardsticks against which the performance of various systems is evaluated. While we agree that analysis of such accidents is an important check upon the general safety of reactor designs, we are concerned that other types of possible accidents may consequently receive insufficient attention in design, construction, licensing, and operation.

B. Primary Engineered Safety Features

In our study, we centered much attention on the "engineered safety features". Because these features are not used in normal operation but are specifically intended to prevent an abnormal incident from becoming an accident, there is only limited operating experience with them. In addition, because of the complexity of the phenomena involved, these features are very difficult to simulate on a computer or to test in simulated accident conditions. Therefore, there is a lack of well-quantified understanding of the performance of some of these special systems under some severe accident conditions.

One of the most important of the engineered safety features is the fast-acting SCRAM system for shutting down the chain reaction in the event of an emergency. Certain transients which are anticipated to occur from time to time (pressure, temperature, reactivity) might play an important role in accident initiation. It is very important to shut down the chain reaction during a large transient. While the SCRAM designs, as now prescribed, seem to us to be highly reliable, not enough is known about the effects of transients in the extremely unlikely event that the reactor does not SCRAM. We believe that insufficient attention has been given to the analysis of transients, although it is encouraging that these areas are now being given intensive study. In addition, we are concerned about transient behavior which might occur simultaneously with a massive electrical failure. While there are redundant off-site power sources, the emergency on-site (diesel) power sources are a recognized weak point.

The emergency core cooling system (ECCS) is the engineered safety feature that has received the most publicity, attention, and research. The ECCS is intended to provide emergency cooling to prevent the reactor fuel from melting or losing structural integrity in the event there is a loss of primary system fluid.

We have no reason to doubt that the ECCS will function as designed under most circumstances requiring its use. However, no comprehensive, thoroughly quantitative basis now exists for evaluating ECCS performance, because of inadequacies in the present data base and calculational codes. In addition, it is not clear that the present approximate calculations, even though based on generally conservative detailed assumptions, will in all cases yield conservative assessments of ECCS performance.

We have examined the AEC reactor safety research program intended to resolve these uncertainties. Expanded experimental tests and advanced calculational code development are now under way, with the goal of accomplishing a sufficient quantitative comparison between calculation and experiment so that the technical community can reach consensus on ECCS effectiveness. That consensus can only be reached through several years of effort, using improved research techniques, and with more open publication and review of the results. We doubt that a complete quantitative evaluation of ECCS effectiveness can be achieved through the present program. We recommend below several possible approaches for improvement.

C. Accident Containment and Consequences

The last line of defense in preventing or mitigating the release of radioactivity is a further set of engineered safety features designed as a backstop in case of significant failure of the preceding safety features. The greater part of this last safety umbrella is the containment machinery and building which encloses the entire reactor primary system. These containments, which have worked well in controlling routine and minor radioactive emissions, have not yet been subjected to test by a large-scale controlled or accidental release. More research toward increasing the effectiveness of containment devices would be prudent, along with more vigorous pursuit of the possibilities for major improvements in containment design.

Although a major release of radioactivity is unlikely, it is important to calculate the types and extent of consequences of releases under various circumstances. We have found that these calculations are very difficult. There are significant uncertainties in nearly every category of potential consequences: acute deaths, latent cancers, and property damage/denial. We have made no independent studies of acute effects, the estimates of which are particularly dependent upon details of local siting, weather, and population, and upon important uncertainties in acute biological effects of radiation. However, for the same releases and the same basic references for the biological effects as taken in Draft WASH-1400, we estimate substantially larger long-term consequences, particularly concerning land damage/denial and possible latent cancers from exposures to individuals who live in areas which are contaminated below the evacuation thresholds used in Draft WASH-1400.* The social significance of the long-term consequences depends in part upon the probability of the assumed release, regarding which we have made no independent assessment. However, the uncertainties in estimates of consequences need to be resolved because they have important implications in reactor design, siting policy, and protection against potential sabotage. In analyzing the societal risk-benefit balance of commercial nuclear reactors, one must be able to estimate with reasonable confidence both the probability and consequences of system failure; research must continue on both.

Considering the great social importance of reactor safety and the large present and future capital investment in light-water reactors, the current funding of safety research is relatively small. We believe that the many technological opportunities for the enhancement of reactor safety warrant the investment of additional funds in safety research.

---

* We understand that substantial revisions are being considered before publication of the final WASH-1400 report (private communication, NRC, 17 March 1975).

D. Major Recommendations

Many recommendations are made in the body of this Report. A few of the major ones are summarized here, but in each case the reader is referred to the main text for detailed discussions of the background and rationale. Our major recommendations, which have not been ranked according to their importance, include the following:

1) Human engineering of reactor controls, which might significantly reduce the chance of operator errors should be improved. We also encourage the automation of more control functions and increased operator training with simulators, especially in accident-simulation mode.

2) Measures should be taken to quantify the effectiveness of the present quality assurance program, using both the analysis of experience already reported and new measurements on the quality assurance system.

3) The techniques used in Draft WASH-1400 for the calculation of accident sequences and their probabilities should be:

- employed to estimate quantitatively whether assumed subsystem failure data are compatible with the observed individual small accidents;
- used to provide parametric studies of the effects of phenomena which are ill-understood in the identified sequences;
- refined so that they can be used for continuing risk assessment on a routine basis with a growing data base of failure data.

4) The Draft WASH-1400 analysis of accident consequences should be redone taking into account the modifications discussed in our report, in order to obtain corrected consequence estimates. The results will help to determine the magnitude of the benefits which might be obtained from the introductions of design changes and means of consequence mitigation.

5) The problem of sabotage and its effect on increasing the risk of radioactivity release should be studied carefully. We have no way of estimating the present likelihood of sabotage; however, we believe that reactor security can be improved and have specific recommendations for studies that go beyond those already underway.

6) The ECCS safety margin should be quantified, and if necessary, improved through one or more of the following approaches:

- the substitution of more easily analyzable or more effective ECCS concepts;
- a much stronger theoretical and calculational development effort combined with a much improved experimental program, the results of which must be published openly for evaluation by the technical community;
- a series of large-scale experiments along with some standardization of reactors. Detailed planning and analysis for this approach should begin immediately in case it should be decided in the future that it is needed.

There should be increased emphasis on realistic calculations and experiments as opposed to those which merely attempt to set upper limits on the behavior of a reactor in an accident. In view of the number of reactors now operating and being planned, we believe it is important that the reactor safety research program quickly take major steps to bring about a convincing resolution of the uncertainties in EECS performance.

7) In the area of safety research, more emphasis should be placed on seeking improvements in containment methods and technology. In particular, controlled venting of the containment building in case of overpressure should be studied. A careful assessment should also be made of the benefits and costs of alternative siting policies, such as remote, underground, and nuclear-park siting.

8) There should be more effort to resolve major uncertainties in estimating consequences, including improvement of the biological-effects data base. Techniques for mitigation of consequences should be developed, especially in connection with the problems of decontamination after a large accident.

9) While we strongly endorse the substantial improvements that have been made in the safety research programs and in the openness to scrutiny by the technical public in the last two years, additional measures should be taken to continue to improve the research program and techniques and to assure that the results of both experimental and computer code development work related to safety are openly published.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

1039

NOV 1 9 1976

MEMORANDUM FOR Ben C. Rusche, Director
Office of Nuclear Reactor Regulation

FROM Evangelos Marinos, Reactor Engineer
Electrical, Instrumentation & Control Systems Branch

SUBJECT RESOLUTION OF TECHNICAL ISSUES

In response to your memorandum to the NRR staff dated November 3, 1976, and your memorandum to me dated November 12, 1976, I have made an attempt to provide a timely response to your requests. The attachment herewith includes my knowledge on issues 4, 5, 9, 10, and 12 included in your memorandum of November 3, 1976 and other concerns expressed by me in the past, some of which are briefly addressed in a memorandum to T. J. McTiernan from Roger Fortuna and William Foster, dated November 8, 1976.

Admittedly my discussion of the issues included herewith may not be totally comprehensible, however, it is the best effort I could make under the time constraints imposed upon me for responding to your request. I will be happy to discuss these issues at any length with members of the staff and the ACRS.

I further should like to point out that in view of time constraints I have limited my responses to issues that I am most familiar with. I share, however, the concerns expressed by my colleagues and could provide constructive comments on those concerns if time permitted.

Evangelos C. Marinos

Evangelos Marinos, Reactor Engineer
Electrical, Instrumentation &
Control Systems Branch

Enclosure:
As stated

cc: R. E. Heineman
T. J. McTiernan

ATTACHMENT I

Attachment to November 19, 1976 Memorandum
From E. C. Marinos to Ben C. Rusche, Director, ONRR

A. The following are my responses to issues 4, 5, 9, 10 and 12 included in memorandum to NRR staff, dated November 3, 1976:

1. Issue No. 4 - Loss of Offsite Power Subsequent to Manual Safety Injection Reset Following a LOCA

   This issue I believe is stated incorrectly because of the following:

   a) The reset feature of the Safety Injection System (SIS) signal is not unique to Westinghouse ECCS designs, other designs possess the same feature.

   b) The operator does not only have the capability to reset, he is required by emergency procedures to perform this reset function immediately after the prescribed equipment time delay, which is set between (0-3) minutes for Westinghouse plants.

   c) The staff has not consciously accepted this feature with this inherent design deficiency (of loss of all motive power after reset, or before reset), it merely was never recognized in the past. A review reminder issued to the EI&CSB, dated April 4, 1974 informed the members of the branch that they should pursue the consequences resulting from the loss (interruption) of power to ESF any time during the accident sequence.

   d) The thermo-hydraulic effects on the core cooling have not been considered when flow to the core has been interrupted (for an interval of time) at any time during the accident sequence.

   e) The staff has not carefully reviewed, in all cases, the proper loading of the diesel generators after (SIS) reset for operating plants and many plants under review in the CP and OL stage, because staff members were not permitted to question applicants on this issue.

   In conclusion, I believe that since the staff has not carefully considered the consequences of loss of core cooling in the injection phase during accident conditions, additional ECCS evaluations should be conducted to assess its effects on the core. Furthermore, the staff should not rely on manual reinitiation of safety injection at any time during the injection phase, since it is not possible to accurately determine the operator response in a given time interval, unless this interval is greater than ten minutes after loss of offsite power has occurred.

In my discussion with members of Reactor Systems Branch (Zoltan Rosztoczy) I was informed that ECCS evaluations had been completed by the staff and that interruption of flow to the core had not been considered during any part of the accident sequence.

2. Issue No. 5 - Analysis of Postulated Reactor Coolant Pump Rotor Seizure Incident

The staff has required that the pump seizure event be re-analyzed assuming loss of offsite power and coastdown of the undamaged pumps. A meeting was held with Westinghouse on the subject, on May 18, 1976 and Reactor Systems Branch was expected to evaluate Westinghouse's submittal. To my knowledge other nuclear steam suppliers have not been asked to conduct similar re-analyses.

In conclusion, I believe that the staff should evaluate the pump seizure event with coastdown of the undamaged pumps. Furthermore, if applicants and licensees elect to retain the fast transfer feature (of reactor coolant pumps) from the unit auxiliary transformer to the startup transformer, for this and other events that result in Main Turbine trip, the staff should include in their safety review the evaluation of this transfer feature. In addition the staff should evaluate the provisions made in the designs to assure that reactor coolant pump motor damage will not occur (causing rapid loss of reactor coolant flow) from overvoltage impressed on the motor due to improper phase-relationship between the transferred power source and the residual motor emf.

3. Issue No. 9 - Frequency Decay

Westinghouse in an attempt to resolve this issue generically submitted a Topical Report (WCAP-8424) on the subject, and I was assigned the task to evaluate the submittal. My evaluation revealed that plant initial conditions assumed in the topical were not complete. Therefore, Westinghouse was requested (by letter dated October 6, 1975) to amend its report to include in its calculations conditions identified and used by the staff in the staff's independent evaluation, which revealed frequency decay rates considerably in excess of those claimed in the topical report. Subsequent to that Westinghouse has confirmed the staff's evaluation and elected to withdraw its position in the topical, and refer the issue for resolution by applicants on a case by case basis.

Incidentally our evaluation has further revealed that plants operating at low power levels will experience greater frequency decay rates as opposed to plants that operate at peak power levels. Therefore, it may not be desirable to impose peak power restrictions as your memorandum to the staff indicates for a possible requirement.

I reported to my supervisor the following results:

a) The accident analysis does not provide a basis for selection of underfrequency reactor trip set points and time delays, associated with this protection. Therefore, we cannot conclude that this protection is adequate.

b) The reactor trip is not directly derived from the variable monitored. Opening of reactor coolant pump breakers generate reactor trip which is in violation of protection criterion (IEEE-279).

c) Possible frequency decay rates have not been evaluated. Therefore, 7Hz/sec decay rates could not be accepted as conservative rates for this plant design, as the original writing of the NRC response claimed as acceptable rate. However, this original writing (see attachment II) was not incorporated in the final response to the Joint Committee on Atomic Energy.

The final response of the NRC testimony has not included any of the points discussed in items a, b, and c above. Additional discussion on this issue is included in item A3 of this attachment.

2. Grid Stability for Indian Point Units 2 and 3

I believe this issue has been adequately addressed in the memorandum from Roger Fortuna and William Foster to T. J. McTiernan dated November 8, 1976, therefore I have no additional clarifying comments to make on this subject. However, additional discussion is included in item A4 of this attachment.

3. Electrical Penetration of Reactor Containment

When I was assigned to prepare a response to the allegations made by the ex-General Electric employees (that the containment penetrations do not receive adequate attention by the NRC staff) I expressed my general agreement with this allegation and I asked my supervisor to include in the final response to that allegation the comments prepared by me on the IEEE Std-317 and the Regulatory Guide 1.63, included in a memorandum from R. L. Tedesco to Guy A. Arlotto dated February 4, 1976. Of the four comments included in that memorandum however, only the least significant was included in the final writing that was submitted to the Joint Committee on Atomic Energy. The staff further concluded that penetrations do receive adequate attention by the staff.

The staff's acceptance of electrical penetrations is limited to applicant's identification of criteria used in qualifying these penetrations. Specific design and qualification parameters are not identified neither requested by the staff.

In concluson, I believe that the staff should utilize the qualification criteria set forth by the IEEE Std-317, 1975 including the comments made by the staff to evaluate the adequacy of the electrical penetrations for current applications and operating plants. For the case of operating plants, prototype testing of penetrations used would provide adequate information to assess acceptability of presently installed units.

1040

Issue No. 4

Loss of Offsite Power Subsequent to Manual Safety Injection Reset Following A LOCA

This issue is defined as follows:

> "The ECCS designs are such that beginning about two minutes after occurrence of a LOCA the operator is required to reset the Safety Injection System (SIS) signal. If the operator does reset the SIS signal (a few minutes after LOCA) and if a loss of offsite power should then occur, prompt operator action would be required to restart the LOCA loads. The logic for startup of the emergency diesel generators would cause automatic sequencing to pick up the normal shutdown cooling loads in some designs and in others no loads would be sequenced (since there would be no accident signal present) rather than the LOCA loads, which would be the case if SIS had not been reset. The staff has accepted this design, in some plants provided that procedures for use of the SIS reset, and for actions required in the event of loss of offsite power after SIS reset to sequence on the proper loads without overloading the diesels, are carefully reviewed for adequacy.
>
> "The staff also should consider the effects on the core of loss of power to engineered safety features following a LOCA and after safety injection signal reset.
>
> "The resolution of this issue should be implemented on all plants."

The essence of this issue is whether the loss of offsite power (LOP) should be assumed to occur at any time following a loss-of-coolant accident (LOCA) or only simultaneously with a LOCA as is now assumed.

The original issue was the possibility that the Safety Injection System (SIS) Signal would be reset manually by the operator only a short time after the occurrence of a LOCA, and that a subsequent LOP could lead to conditions that would impair the operation of the Emergency Core Cooling System (ECCS). This concern was addressed specifically in the NRC Staff

Issue No. 4

response by

reset of the

by further r

These propos

by the minor

The ACRS bel

primarily in

in emergency

to the orig

whether the

analyses.

following a

the diesel

The failure

can be just

(1)

(2)

(3)

The NRC St

was impos

failures

seem to b

LOCA) aft

response by proposing changes in plant emergency procedures to prohibit reset of the SIS signal earlier than 10 minutes after a LOCA signal and by further reviews of plant design features and emergency procedures. These proposals seemed to result directly from the concerns expressed by the minority group.

The ACRS believes that the actions proposed by the NRC Staff, which primarily involve procedures but which in some cases may require changes in emergency diesel loading sequences, represent an acceptable response to the original concerns. However, there still remains a question of whether the LOP subsequent to a LOCA should be considered in the accident analyses. This concern exists whether or not the SIS signal is reset following a LOCA signal, since a LOP would require transfer of loads to the diesel generators. This transfer may affect the efficacy of the ECCS.

The failure to consider LOP at any time following a postulated LOCA can be justified on any of three grounds:

(1) It is impossible.

(2) It has a sufficiently low probability.

(3) It does not lead to unacceptable consequences.

The NRC Staff made no attempt to prove that the LOP at a subsequent time was impossible. The Staff did present estimates of probabilities of random failures of the power grid leading to LOP. These probabilities would seem to be applicable to the period (10 minutes or more following a LOCA) after which the SIS signal could be reset. They do not address the probability of LOP as a consequence of the LOCA itself (e.g., grid instability due to turbine trip) or as a consequence of the same event as that causing the LOCA (e.g., earthquake).

Some calculations were presented by the NRC Staff to show that the ECCS cooling capability would not be degraded as a result of a subsequent LOP. These calculations, however, had been made only recently and applied to only one plant. Similar calculations of a more general nature should be made, taking into account possible variations in plant configurations and parameters as well as possible variations in diesel-loading sequences, if it is desired to present conclusive evidence regarding the acceptability of the consequences of the postulated loss of power.

The ACRS believes that a sufficient basis does not now exist to eliminate from consideration the LOP at any time subsequent to the occurrence of a LOCA, and recommends that further studies of the probabilities and consequences of such an event be made by the NRC Staff. The ACRS believes further that the several actions proposed by the NRC Staff constitute an acceptable interim solution and that, in view of these actions, there is no need for any immediate changes to existing operating licenses beyond those required to implement the Staff's proposed actions.

Central File
1043

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

April 26, 1978

MEMORANDUM FOR: Lee V. Gossick
Executive Director for Operations

FROM: Stephen H. Hanauer, TA EDO

SUBJECT: FEEDBACK OF INFORMATION INTO THE REACTOR REGULATION PROCESS

Enclosed you will find a copy of a thinking paper on the captioned subject. The basic conclusion I have come to is that the feedback of operating and research information into the reactor licensing process can and should be improved. More detailed recommendations are given in Section 8 of the enclosed paper.

A draft paper was circulated. NRR does not agree with the thrust of this paper, believing that "problems are identified and promptly reported." Mr. Case's memo is enclosed. I have taken some of his comments into account, but the disagreement remains.

IE agrees with the thrust of this paper, but recommends a separate, independent Office of Operations Evaluation. Mr. Jordan's memo is enclosed.

Stephen H. Hanauer
Technical Advisor to
Executive Director for Operations

Enclosures:
1. Paper on "Feedback of Information Into the Reactor Regulation Process"
2. E. Case memo dtd 4/3/78
3. E. Jordan memo dtd 3/24/78

cc: w/encls.
W. Dircks
E. Case
S. Levine
R. Minogue
E. Volgenau
C. Smith
A. Buhl
R. Moore
R. Hartfield
N. Haller

TA EDO SHH
SHHanauer:mc
4/26/78

OHM-3
Lic-Regulation

FEEDBACK OF INFORMATION
INTO THE REACTOR REGULATION PROCESS

Stephen H. Hanauer
March 31, 1978

1. Introduction

This paper deals with the use of information from operation and research to feed back into the licensing, standards, and inspection of current and future facilities. The present paper deals with power reactor safety only; the potential for extension to other NRC regulatory programs needs further study.

2. Sources of Information

In this paper, "information" is used in a braod sense to include the technical content of operating experience, research and development results, inspection experience, experience in the licensing process and in applying codes, standards, and guides, and other sources.

The applicant has the primary responsibility to supply the information needed to justify the safety of his proposed operation; that information is not the subject of this paper. The NRC has to review the applicants' proposals, using the applicants' and all other available relevant information in making licensing decisions. In addition, the NRC must maintain surveillance over licensees throughout the construction, useful life, and decommissioning of the licensed activity, and codify its practice in regulations, standards, and guides - all these activities to be carried out in the light of all available relevant information.

Both research activities and the ongoing licensee construction and operation programs are sources of information potentially important to NRC regulatory programs.

3. Functions Related to Information Feedback

The functions involved in the feedback of this information into the NRC programs are described in the following paragraphs.

(1) Collection and organization of the information; indexing and classifying its content; storing it in a retrievable and analyzable form.

(2) Dissemination of unanalyzed data periodically and on demand, cut and organized in various potentially useful forms.

(3) Evaluation of significance; in particular, identification of items needing non-routine attention or action. To the extent practical, criteria are used for such screening (e.g., criteria for Abnormal

Occurrences), but judgment must be applied. The Reactor Safety Study is beginning to be used to evaluate the significance of some items in terms of risk.

(4) Development of technical and statistical inferences, such as

Trends
Outliers
Problem areas
Little things that add up
Poor performance in some particular
area or by some particular organization.

(5) Application to licensing decisions (including backfitting), standards, and inspections.

The emphasis in the feedback function is on judgment, based on the incoming information. Ideally, the process requires sufficiency and validity of the information, technical and statistical competence in inference, evaluation and judgment in application; practically, these requirements are fulfilled to some degree short of perfection. The objective is to draw valid conclusions leading to action where appropriate.

4. Relationship to Probabilistic Analysis

Information feedback would be needed even if probabilistic analysis (PA) didn't exist. The Reactor Safety Study and other developed tools for PA allow a precision of analysis that is useful where correctly applied.

The evaluative function should be especially sensitive to the potential occurrence of sequences and failure modes likely to be missed or misinterpreted, and those that are difficult to include in PA, such as human error, system interactions, common mode failures, design and manufacturing errors, consequential failures.

5. Present Picture - Operating Information

The present setup is partly described in SECY-77-229 dated May 4, 1977. This presents the IE program to screen and evaluate information, and pass it on to NRR, and the NRR program to apply it. Salient features are:

(1) The IE Region sieves the incoming information for action items, with the head inspector for each plant responsible for information coming from it. IE-HQ sieves it again for significance

(audit) and generic items. The audit function is in the A/D for Technical Programs, Division of Reactor Operations Inspection. The application of new information into inspection modules is the responsibility of the A/D for Field Coordination in the same division.

(2) Routine and nonroutine information are handled on different time scales, including telephone calls, Preliminary Notifications, Regional Daily Reports, and memoranda as appropriate. IE gets out bulletins and circulars as needed, but this is sometimes delayed by the need for NRR review.

(3) The NRR project managers are initially responsible for incoming information on their plants.

(4) Technical responsibility for information feedback on generic matters is diffused in NRR in the technical branches and technical activities project leaders. There is a framework for Operating Experience Memos, etc., but no centralized group to make sure all significant items get attention. An exception is tracking (in the Pink Book) of the most important items: Transfers of lead responsibility (from IE to NRR) and interoffice action items. MIPC (soon, MPA) has computerized files of LERs and NPRDS.

(5) Some failure data are inherent in the LERs, and other data are being accumulated in NPRDS. The latter is in need of improvement; see the January 16, 1978 report of the NPRDS Working Group.

(6) The role of MIPC in evaluation of operating information is not altogether clear. IE information goes directly to NRR, with MIPC filing LERs and having the lead on AORs. MIPC also handles the NPRDS interface. MIPC disseminates undigested LER and NPRDS information, and also does data file searches, sorts, and some analysis.

(7) The Probabilistic Analysis Staff of RES uses and analyzes operating data, carries out programs of methodological development for data analysis, and helps other offices with special problems.

(8) NRR/DOR issues Operating Experience Memos to other NRR divisions, to forward formal DOR findings on significant safety issues for use in CP and OL reviews.

6. <u>Present Picture - Research Information</u>

The system of Research Information Letters (RILs) described in NUREG-0378 and -0435 is working well in RES, but the most recent

"RIL Book" shows many office responses to be trivial or missing. In some instances, NRR or SD have taken appropriate action, but the RIL book doesn't reflect it. A better system of evaluating the true significance to NRC programs of a completed segment of research (that's what a RIL embodies) is needed.

Since a large fraction of the research program is purely confirmatory, the results can be said just to confirm what we knew all along and to have "no impact" on NRC programs. The writer suggests that this view is incomplete. Presumably, the research was undertaken in response to an agency need; the results are therefore "significant" in fulfilling whatever the need was perceived to be. Confirmation of the correctness of a regulatory program or requirement, or assessment of the margin of safety, is in this context more than "no impact."

If, contrary to the author's perception, a majority of RILs should turn out to have little or no true impact on NRC programs, then those RES programs need reconsideration.

A large number of technical reports come from research programs in addition to RILs. These include quick look reports, periodic progress reports, and topical reports. At present, there is no organized scheme to sieve these for items requiring nonroutine action.

The members of the Research Review Groups appointed by NRR, IE, and SD could be made responsible for this function, but this has not so far been done. To know whether this would be a good idea would require reconsidering the Review Group structure and assignments with this function in mind. Some revised guidelines for NRR participation in Review Groups go part way in this direction; they are given in an E. G. Case memo dated March 14, 1978.

The Research Analysis Branch in NRR could serve as a centralized organization to make sure all reports are sieved, but does not now do so.

7. Conclusions

(1) Operating information flow seems not bad.

(2) Little statistical and technical study is given the great mass of operating information. MIPC has a small program. I think more is needed; in particular, a more systematic approach and more nearly adequate resources.

(3) Plant-specific operating information is sieved by designated cognizant individuals in IE and NRR.

(4) Recognition and action on generic items of operating information is assigned to a small audit group in IE. In NRR, the assignment is diffused except for Pink Book or Generic Task items.

(5) Research information generation and dissemination are good.

(6) Office response to research information is varied for RILs and not assigned for non-RIL reports.

8. Recommendations

(1) Give one or more specific organizations in NRR, and other user offices, the responsibility for assuring that incoming non-plant-specific operating information and all research information are sieved for items requiring nonroutine action, so as to focus the responsibility now diffused by "making everybody responsible."

(2) Resource allocations should be made for feedback functions that are necessary; this is not now done throughout the agency.

(3) Put a time limit on how long NRR can delay an IE circular or bulletin.

(4) Expand the technical and statistical study of operating information. This could be assigned to MIPC or DOR or a separate OOE. I do not believe that putting it in DOR is "setting the fox to guard the henhouse." This is not, in my opinion, an audit or QA function on NRR or DOR, but information analysis for feedback. I am not recommending an "information czar." I note that IE, in comments on a draft of this paper, recommends "a separate, independent OOE to assure evaluation and feedback to all NRC organizations," and that others have recommended some degree of independence. A previous OOE in IE was discontinued not long ago.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

APR 0 3 1978

MEMORANDUM FOR: Stephen H. Hanauer
Technical Advisor to
Executive Director for Operations

FROM: Edson G. Case, Acting Director
Office of Nuclear Reactor Regulation

SUBJECT: THINKING PAPER ON INFORMATION FEEDBACK

I have had the Division Directors review your proposed paper. In general, we feel that the identification facet is adequate. Through the LER system, research program and Part 21 reports, problems are identified and promptly reported. Whatever new system comes from your proposal should acknowledge this fact.

The timing of staff responses to safety issues could use some improvement. The Technical Activities Program is an attempt to get the staff to respond to problems and resolve them in a timely manner. More effort should be applied to this aspect could result in some improvements. Because of budget limitations, not all of the 500-600 research reports are sieved in NRR. Many, such as semiscale, ECCS bypass, and Frankfort containment tests are.

Other comments are provided in the enclosure.

Edson G. Case, Acting Director
Office of Nuclear Reactor Regulation

Enclosure:
As stated

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

MAR 1 0 1978

MEMORANDUM FOR D. Crutchfield
Program Support Branch, ONRR

FROM Roger J. Mattson, Director
Division of Systems Safety

SUBJECT FEEDBACK OF INFORMATION INTO THE REACTOR REGULATION PROCESS (DRAFT HANAUER MEMO)

The Hanauer memo is based on the premise that feedback of information from research and from construction and operation experience of nuclear power plants into the regulatory process is inadequate. With regard to the first part of the feedback process, recognition of problems, the premise is incorrect. My view is that through such programs as licensee event reporting, Part 21, and NRC research, we have a myriad of identification mechanisms for safety problems. The proposal seeks to organize this recognition phase into a more structured system. The system we have is loose and diffuse, but it seems to work. Its efficiency is doubtful, so some more careful attention to the overall structure is probably a good idea. Although Hanauer states that he does not recommend establishing an "information czar" his recommendations would tend to effect such a result. I believe that the recognition, identification and reporting of safety problems is the responsibility of all of the staff and that individuals in the various organizations are the best qualified to recognize the potential safety issues in their areas. Whatever new system of information control we adopt, it should take advantage of this fact.

The second part of the premise, action in resolving problems, is a problem. The examples of lag, delay, contention, inaction, indecision, and all of the other bureaucratic ills are many and painful; viz fire protection, ATWS, equipment qualification, overpressure. While recognized early, action in resolving these issues has been untimely. The Technical Activities Program is one attempt to manage and improve our response to new safety issues. Another is the Topical Report Program. Some programs aimed at discovering problems, such as research, have a disproportionate share of the resources. A striking new example of this is a $13 million research program to improve safety which has not been shown to be necessary while the TAP schedules slip because of insufficient resources. The programs that address solutions, the Technical Activities

Program, the Technical Assistance Program, the Topical Report Program have too small a share of the resources. Although research is being redirected and work on the others is gathering momentum, the necessary reallocation of resources is far from being accomplished. Rather than institute another program to identify problems, such as suggested by Hanauer's paper, the programs to solve the problems we have already identified need to be given the highest priority.

A markedup copy of your request for comments is attached.

Roger J. Mattson

Roger J. Mattson, Director
Division of Systems Safety

Enclosure:
As stated

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

March 10, 1978

Note to W. Dircks
E. Case
S. Levine
R. Minogue
E. Volgenau

Enclosed is a draft memo to Mr. Gossick on "Feedback of Information Into the Reactor Regulation Process." Your comments are solicited, and should be received by me before COB March 24 to be included in the final version.

Stephen H. Hanauer
Technical Advisor to
Executive Director for Operations

Enclosure:
Draft - Feedback of Info
into the Reactor Regulation
Process

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

MAR 24 1978

MEMORANDUM FOR: Stephen H. Hanauer, Technical Advisor to Executive Director for Operations

FROM: E. L. Jordan, Executive Officer for Operations Support, IE

SUBJECT: FEEDBACK OF INFORMATION INTO THE REACTOR REGULATION PROCESS

This is in response to your March 10, 1978 memo to Ernst Volgenau on the captioned subject.

Enclosed are our comments on the draft paper. In commenting we have provided our thinking on the need for an improved NRC feedback system. Also, we have briefly described IE's present feedback from inspection activities and related programs under development.

We have no basic disagreement with the need or objectives discussed in the paper. Our problem continues to be one of finding sufficient resources to adequately perform information evaluation and feedback.

In our view, we concur with recommendations (4) and (5) combined with a separate, independent OOE to assure evaluation and feedback to all NRC organizations.

Thank you for the opportunity to comment.

E L Jordan

E. L. Jordan, Executive Officer
for Operations Support, IE

Enclosure:
As stated

cc: J. G. Davis
H. D. Thornburg
N. C. Moseley

Feedback Of Information Into Reactor Regulation Process

We agree with the idea that NRC should study a system for feedback of experience[1/] to the regulatory program. We have or are currently developing systems to feedback inspection experience to the inspection program, enforcement program, to the licensing programs, and to standards development. Inputs start at the inspector level and continue through the headquarters level. The IE Headquarters Divisions evaluate the feed back and initiate appropriate action with NRC counterpart organizations. The evidence of these activities is: IE Bulletins and Circulars; memoranda to the offices with licensing responsibility regarding license provisions, safety matters, and generic problems; input to standards review; initiation of a program for systematic comments from the field on Regulatory Guides, evolution of the inspection enforcement programs, etc.

We are actively pursuing licensee performance evaluation and plan to have a strong emphasis on performance evaluation in connection with the forthcoming Resident Inspector Program. The primary emphasis will be on licensee performance evaluation with attention to IE program performance and inspector objectivity. These efforts will be based on the existing information system and other safety inputs that

1/For this purpose we define experience in a broad sense, including nuclear power plant operating experience, research results, results of development, inspection experience, licensing experience, experience in the application of codes, guides and standards, and other information collected that is related to nuclear safety.

reflect or provide insights into licensee performance, IE performance, or inspector performance. Feedback from the system you describe would be utilized in our appraisal efforts.

We believe that the NRC presently has a reasonable system for responding to the first order aspects of incidents, occurrences, and other problems that arise. The inputs can be made at various levels of the NRC organization, evaluations are made, and response actions are taken. The system isn't completely formalized but it works.

The system you refer to we regard as a system for responding to the second order effects of operating experience. As second order effects we include: system and component reliability performance analysis, verification of safety assumptions, single failure assessment and validity assessment, accident probability assessment and analysis, identification of new accidents, etc. We agree that there is a need to study and improve NRC systems in this area.

We believe that it can and must be done; however, we believe that it will be difficult to do so. Presently the information system has some holes (reliability data) and needs discipline (It is difficult to retrieve desired information cut in several different ways.). We are in the early stages of the development and use of probabilistic safety analysis and must depend on deterministic methods which rely on technical judgement. Probabilistic analysis has the potential for providing a logic for safety analysis.

We believe that attention should be given to the matter of the "fox in the hen house" in the final implementation of what we consider to be a portion of the total NRC feedback and response system.

We have a considerable interest in this matter because we believe that can lead to enhancement for public safety. We see our role in second order feedback as follows:

- Make inputs based on field experience and considered analysis of performance analysis data.
- Verify and/or followup on matters identified for field inspection by those responsible for analysis data.
- Act on the results of feedback analysis and use those results in the inspection program.

66 350 NSIC Response to Item 1, Attachment 7

Parler's copy

9/16/71 EX 1042 1044

UNITED STATES OF AMERICA
A/CONF.49/P/016

TECHNICAL SAFETY ISSUES FOR LARGE NUCLEAR POWER PLANTS

S.H. HANAUER, P.A. MORRIS
U.S. Atomic Energy Commission, Washington, D.C.,
United States of America

Abstract–Résumé–Аннотация–Resumen

TECHNICAL SAFETY ISSUES FOR LARGE NUCLEAR POWER PLANTS.

Although the basic requirements for and means of achieving reactor safety remain unchanged, much has been learned from research and development projects and from analysis and experience in the design, construction, and operation of power reactors. Safety reviews within the past few years by applicants and the USAEC regulatory staff, together with the USAEC Advisory Committee on Reactor Safeguards, have resulted in a number of changes in plant design or operation. This paper discusses some of the most significant of these changes and the reasons for them. Examples are given that relate to site and environmental characteristics, reactor design, coolant-system design and performance, design of the containment and other structures, design and performance of engineered safety features, instrumentation and power-system design, and quality-assurance procedures. Although much progress has been made in reactor safety, more remains to be done. Experience with and analysis of actual systems uncover new safety issues and new aspects of old safety issues that require further study and resolution. Some of the most important such technical safety issues currently under consideration are discussed. One of the most challenging questions is the appropriate balancing of risk and benefit. For the safety reviewer, this means establishing acceptable risks for accidents and anticipated operational occurrences and therefore reliability criteria for protective systems and engineered safety features. Available technology and information are reviewed, and principles are stated for considering risk analysis in the absence of adequate data. The performance of protective systems and engineered safety features must be considered as well as their reliability. Protective systems whose performance is studied include the reactor-protection instrumentation system, the emergency-core-cooling system, systems to control combustible gas mixtures in the containment, and systems to control the radioactivity in liquid and gaseous effluents. It is becoming evident that human errors and common-mode failures of redundant elements may be the principal causes of protective-system failure. The use of various types of diversity is discussed.

DONNEES TECHNIQUES RELATIVES A LA SECURITE DES REACTEURS NUCLEAIRES DE GRANDE PUISSANCE.

Bien que les méthodes et les données fondamentales pour assurer la sécurité des réacteurs n'aient pas changé, une information considérable a été acquise grâce aux projets de recherche et de développement et au cours de l'analyse de la construction et du fonctionnement des réacteurs de puissance. Au cours de ces dernières années, les rapports sur la sécurité des réacteurs, établis par les équipes projetant la construction de nouveaux réacteurs, par les responsables de la réglementation à l'USAEC et par le Comité consultatif sur la sécurité des piles de l'USAEC, ont abouti à un grand nombre de changements dans la construction et l'exploitation des réacteurs. Le mémoire discute les changements les plus importants et les raisons qui les ont amenés. Des exemples sont donnés qui ont trait aux caractéristiques du site et de l'environnement, à la construction du réacteur, à la construction et au fonctionnement du système de refroidissement, à la construction de l'enceinte étanche et d'autres structures, à la construction et au fonctionnement des dispositifs de sécurité, à l'instrumentation, aux dispositifs de puissance, et aux méthodes pour maintenir la qualité du matériel. Bien que la sécurité des réacteurs ait considérablement progressé, il reste encore beaucoup à faire. L'un des problèmes les plus épineux est d'équilibrer les risques et les avantages. Pour l'examen de la sécurité cela signifie qu'il faut définir des risques acceptables d'accident et autres événements pouvant se produire au cours de l'exploitation, et par conséquent des critères de sécurité de fonctionnement pour les dispositifs de protection et les systèmes de sécurité. Les informations et techniques disponibles sont examinées et les principes d'une analyse des risques, en l'absence de données suffisantes, sont établis. Le fonctionnement des systèmes de protection et des dispositifs de sécurité doit être examiné, ainsi que leur sûreté. Les systèmes de protection dont le fonctionnement est étudié comprennent l'instrumentation pour la protection des réacteurs, les systèmes de refroidissement du cœur en cas d'accident, les dispositifs pour le contrôle des mélanges gazeux inflammables dans l'enceinte étanche et les systèmes de

contrôle de la radioactivité des effluents gazeux et liquides. Il devient évident que les erreurs humaines et les pannes ordinaires des dispositifs sont les causes principales de faillite du système de sécurité. L'utilisation de plusieurs types de dispositifs est discutée.

ТЕХНИЧЕСКИЕ АСПЕКТЫ БЕЗОПАСНОСТИ КРУПНЫХ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ.

Несмотря на то что основные требования и средства по обеспечению безопасности реактора остаются неизменными, осуществление исследовательских и опытно-конструкторских проектов, а также проведение анализа и приобретения опыта в области проектирования, строительства и эксплуатации энергетических реакторов позволили узнать много нового. Результатом изучения вопросов безопасности, проводившимся в течение последних нескольких лет предприятиями и законодательными органами КАЭ США, совместно с Консультативным комитетом КАЭ США по гарантиям безопасности реакторов, явился ряд изменений в конструкции и в порядке эксплуатации установок. В докладе рассматриваются некоторые из наиболее существенных изменений и причины их внедрения. Приводятся примеры, касающиеся характеристик площадок для строительства и окружающей среды, конструкции реактора, конструкции и работы системы теплоносителя, конструкции защитной оболочки реактора и других конструкций, особенностей конструкций и безопасности их работы, конструкции контрольно-измерительной аппаратуры и энергосиловой системы, а также методов проверки качества. Несмотря на то что уже достигнут значительный прогресс в области безопасности реакторов, многое еще остается сделать. Опыт работы и анализ существующих систем раскрывают новые проблемы обеспечения безопасности и новые аспекты старых направлений в этой области, которые требуют своего дальнейшего изучения и решения. В докладе затрагивается ряд наиболее важных технических аспектов безопасности, находящихся в настоящее время в стадии рассмотрения. Одним из самых важных вопросов является соответствующее сопоставление риска и выгоды. Для человека, занимающегося вопросами безопасности, это означает установление приемлемых рисков в случае аварий и возможных эксплуатационных случайностей, а потому и критериев надежности защитных систем и технических аспектов безопасности. Рассматривается современная технология и имеющаяся информация, излагаются принципы анализа риска в случае отсутствия необходимых данных. Работа защитных систем и технические аспекты безопасности должны рассматриваться вместе с вопросами обеспечения их надежности. Изучаемые защитные системы включают систему контрольно-измерительной аппаратуры по защите реактора, систему аварийного расхолаживания активной зоны реактора, системы для контроля образований горючих газовых смесей под защитной оболочкой реактора, а также системы для контроля радиоактивности в жидких и газовых отходах. Становится очевидным, что ошибки, допускаемые человеком, и общие неполадки у многочисленных элементов могут быть главными причинами выхода из строя системы защиты. Рассматриваются различные виды аварийных ситуаций.

PROBLEMAS TÉCNICOS DE SEGURIDAD EN GRANDES CENTRALES NUCLEARES.

Aunque las condiciones fundamentales y los medios para lograr la seguridad de los reactores permanecen inalterables, se ha progresado mucho gracias a las actividades de investigación y desarrollo y al análisis y experiencia en materia de proyecto, construcción y funcionamiento de reactores de potencia. Los estudios de seguridad realizados durante los últimos años, por los solicitantes de autorizaciones y el personal competente de la USAEC, juntamente con el Comité Consultivo sobre Salvaguardias de Reactores de la USAEC, han dado por resultado una serie de modificaciones en la concepción técnica de las plantas o en su funcionamiento. En la memoria se examinan algunas de las modificaciones más significativas y las razones a que obedecen. Se exponen ejemplos referentes a las características del emplazamiento y del medio ambiente, a las particularidades del reactor, a las características y eficacia del sistema de refrigeración, a las particularidades de la contención y de otras estructuras, al tipo y eficacia de los dispositivos mecánicos de seguridad, a las características del instrumental y de la red eléctrica y a las normas para garantizar la calidad. Aunque se ha avanzado mucho en la seguridad de los reactores, es todavía más lo que queda por hacer. La experiencia adquirida con los sistemas actuales y el análisis de dichos sistemas suscitan nuevos problemas de seguridad y aspectos inéditos de problemas que requieren más amplio estudio y solución. Se pasa revista a algunos de los más importantes problemas técnicos de seguridad actualmente en estudio. Una de las cuestiones más difíciles es conseguir un equilibrio adecuado entre riesgos y beneficios. Para el experto en cuestiones de seguridad, esto significa fijar los riesgos admisibles de accidentes e incidencias previsibles de funcionamiento y, por tanto, establecer los criterios de fiabilidad aplicables a los sistemas de protección y a los dispositivos técnicos de seguridad. Se pasa revista a los conocimientos e información disponibles y se exponen principios para el análisis de riesgos, cuando se carece de datos adecuados. Hay que tener en cuenta la eficacia de los sistemas protectores y de los dispositivos técnicos de seguridad, así como su regularidad funcional. Se estudia la eficacia de los siguientes sistemas protectores: instrumental de protección del reactor, sistema de refrigeración de emergencia del núcleo, sistemas para controlar las mezclas gaseosas combustibles en la

condensadores y sistemas para regular la radiactividad de los efluentes líquidos y gaseosos. Resulta evidente que las causas principales de los fallos de los sistemas protectores son los errores humanos y las averías corrientes de los elementos accesorios. Se estudian, también, varios tipos de diversidad.

1. INTRODUCTION

Reactor safety - the avoidance of undue risk to the public health and safety from the operation of nuclear reactors - involves both technical and nontechnical issues. Setting the goals, numerical or otherwise, for acceptable risk and safety is primarily a social and political task. Translating these goals into criteria against which to evaluate proposals for the design and operation of reactors requires social and technical decisions arrived at with great difficulty. Most of the technical effort in reactor safety evaluation is devoted to a more mundane task: comparison of specific reactors against such criteria. This technical effort is performed principally by the plant owner and operator himself, or through his contractors, since the owner is responsible for the health and safety of the public as well as his employees.

In the United States, as in other countries with nuclear reactors, additional responsibility for the health and safety of the public is held by an agency of government. Such responsibility necessarily involves safety evaluations of the same type--if not of the same scope--as those conducted by the owner. In addition, the government agency plays a major role in the development of the criteria referred to earlier. In this paper the authors discuss some of the more important and interesting technical issues that have come to the attention of the Advisory Committee on Reactor Safeguards and the AEC regulatory staff in the last few years.

Some of the issues discussed are considered to have been resolved; that is, both the criteria and acceptable design approaches to meet them are available. Ideally, experience and measurements will have confirmed the design, construction, and operation of the devices or features involved in such a "resolved issue". By no means all safety issues are in this happy state. Others remain, to a greater or lesser extent, short of complete resolution. Lack of resolution often occurs because of the inevitable time delay between identification of an issue and completion of the work needed to resolve it.

For some kinds of issues, complete resolution is not foreseeable as a practical matter. Such problems usually involve events, or combinations of events, of such low probability that thousands of reactor lifetimes would not be expected to encompass even one observed event. Some postulated occurrences used for reactor safety evaluation fall in this class. Thus, design, construction and operating experiences are not expected to confirm the resolution of this kind of issue.

Such rare postulated events--for example, rupture of a large primary system pipe, or failure of the control rods to insert when needed, or occurrence of a severe earthquake--require careful consideration in reactor safety evaluation even though knowledge about them is and must remain incomplete.

It is such issues as these that constitute the most challenging and difficult portions of safety evaluation. Decisions on such issues necessarily involve judgments that must be made without complete information - judgments, therefore, subject to change as additional knowledge is gained.

This paper discusses the general subject of reactor safety goals and criteria, some examples of technical safety issues that have been resolved and finally, some examples of technical safety issues that are unresolved.

2. REACTOR SAFETY GOALS AND CRITERIA

2.1 Safety Goals

The ultimate reactor safety goal is elimination of risk to the health and safety of the public. The principal potential hazard associated with operation of nuclear reactors lies in the possible release of the radioactivity of the heavy elements and fission products produced in the fuel. The safety goal, therefore, is prevention of the exposure of people to this radioactivity. This goal can be achieved with a high degree of assurance, but not perfectly, since the possibility of fuel failure and consequent release of some radioactivity to the environment cannot be precluded absolutely. The ultimate reactor safety goal is thus theoretically unattainable, and a certain residual risk is unavoidable.

The minimization of risk is a realistic, practical goal, but it introduces a dilemma: What is an acceptably low level of risk? What is the basis for choosing it? Minimization is not enough. By choosing operating parameters with greater conservatism, adding more safety features, using more remote sites, one can obtain at least the illusion of greater safety. This process has no end except diminishing returns, or at worst a decrease in overall safety as a result of overcomplication. What is needed is some delineation of what is enough. The necessarily imperfect goal must be translated into a guide to the designer and the person charged with safety.

The decisions as to what risk is acceptable -- as defined piecemeal in criteria, standards, codes, guides -- have, in the past, been guided largely by experience and judgment. For some aspects of reactor safety, formulation of criteria in this way is a relatively tractable task. For the rare postulated events discussed previously, however, this method of establishing criteria is difficult for two reasons. First, the probability - expected occurrence rate - of these events is far too small to permit the accumulation of experience necessary to proceed in a meaningful way. Second, the possible consequences of some postulated failures are so severe that the whole procedure is not applicable. Accumulation of experience - even if it were possible - is unthinkable for highly unlikely events that might kill or injure a very large number of people. Since the acceptability of nuclear reactors, or anything else, depends on the fact that the unthinkable events are very rare indeed, an alternative must be found for dealing with such events in the establishment of criteria.

2.2 Risk Analysis

A seemingly most attractive method for assessing reactor safety goals and criteria is based on a numerical quantification of risk. In its simplest form, the theory defines risk as the product of the probability of occurrence of an event times the consequence of that event, also suitably quantified. Similar, more complicated methods also have been proposed. The total risk is the sum of the calculated risks for everything that can happen. This approach and others of this nature are not the infinite tasks they would at first sight appear to be. A few events are found to dominate the analysis. For plants to be acceptable, extreme cases o. high probability or (at the other end of the scale) serious consequences must be found to involve a low risk.

The potential advantages of such an approach are obvious. The evaluation automatically emphasizes events that contribute significantly to the risk, which is where the emphasis belongs. No decisions need be made about credibility, since "incredible" events eliminate themselves from consideration by their low risks arising from their low probabilities.

Closely associated with risk evaluation is the technology of reliability analysis, used to predict the required probabilities of occurrence. It is in this area that problems arise, in the authors' opinion, which decrease the utility of risk calculations in reactor safety evaluations. For all its proved worth in many areas of technology, application of probability analysis to the type of rare events considered in nuclear safety involves the following uncertainties: (a) There is little or no concrete evidence that the events under consideration obey the laws of probability that underlie the theory. There is no assurance that accident events are random in time or independent of each other. The intellectually satisfying idea of reliability analysis is no more than a hypothesis for these events; (b) Even if the framework of the theory were correct, the values of the parameters are largely unknown.

The method now generally used to predict these probabilities -- cascading of probabilities of the individual "failures" that make up the event -- is known to be inadequate. The serious or potentially serious events that have occurred have been characterized by concurrent failures, usually interdependent or causally related. Thus the theory's assumption of independence of failures has not been borne out by experience.

Despite these shortcomings, reliability analysis and, to a lesser extent, risk calculation techniques are used in reactor safety evaluation in the United States. In some areas, such as meteorology, there is a substantial body of knowledge to serve as a basis for the calculations; these results are thought to approximate reality. Where the basis is less firm, the calculations are nonetheless useful in making comparisons on a relative basis, as opposed to an absolute basis, thereby directing attention to the more important considerations.

2.3 Design Basis Accidents

The principal tool used in the United States for reactor safety evaluation is not risk calculation but analysis of a spectrum of design basis accidents. The response of the reactor plant to each of these postulated events is predicted and the radiological consequences are compared with arbitrary criteria. Two such criteria are used: one for events expected to occur frequently during the reactor lifetime, the other for very unlikely events. Subdivision of classes of postulated events is surely possible and has been proposed; the present state of knowledge appears inadequate to the authors to justify quantification of intermediate events, but qualitative comparisons appear to be meaningful.

It is evident even from this brief discussion that despite the explicit rejection of quantitative risk analysis for safety evaluation, notions of probability do play an important role. A more careful investigation suggests not two but four classifications of events:

Class 1. Expected occurrences whose effects or consequences must be negligible.

Class 2. Occurrences whose frequency is intermediate between Class 1 and Class 3, that are only beginning to be defined and treated separately.

Class 3. Unlikely severe accidents used for design bases.

Class 4. "Incredible" events against whose consequences no protection is required.

The classification is based on probability, even though the values of the probabilities are not well known. If there is any doubt, an event can be placed in a more probable classification to assure that the evaluation is on the conservative side of reality. The classification scheme is seen to be a crude approximation to risk analysis.

2.4 Defense in Depth

The concept of defense in depth is another way of expressing the foregoing ideas. Reactor designs are required to include a number of barriers between people and the radioactivity contained in the fuel. In water reactors these barriers are the fuel matrix itself, the fuel cladding, the primary system pressure boundary, and the containment. Expected operating transients and other Class 1 events are required not to jeopardize any of the barriers. Any failures in the fuel or its cladding would release radioactivity to the primary system, from which only small leakage would occur; a radioactivity cleanup system would prevent any significant release of radioactivity to the environment. For Class 2 events, and most Class 3 events, engineered safety features protect the primary system, although some of these events could lead to radioactivity releases. Severe postulated breaches of the primary system (the most severe Class 3 events) could lead to rupture of the fuel cladding and release of radioactivity from the fuel and through the breach into the containment; emergency core cooling systems and other engineered safety features would limit the radiological consequences to persons off site.

Class 1 events are expected to happen, so that their consequences must be negligible or nearly so. Practically, the design of features to cope with Class 1 events will be determined by economic considerations. For Class 2 and Class 3 events, the acceptable consequences are progressively more severe commensurate with their lower probabilities. Class 4 events have such low probability that their consequences need not be considered.

The principal defense against accidents is prevention. All structures, systems, and components important to safety must be designed, built, and operated so that the probability of occurrence of an accident is very small. The key to achievement of this objective is an effective quality assurance program, discussed at length elsewhere.[1] However excellent the quality assurance program, it must be acknowledged to be imperfect. Protective systems are installed therefore to deal with such transients and failures as may occur despite all that is done to prevent them. A third echelon of the defense in depth is the engineered safety features designed to cope with unlikely failures that go beyond the capabilities of the accident prevention and protective systems, as well as highly unlikely failures of the other defenses themselves. The designs of engineered safety features are evaluated to provide assurance that they will function properly under accident conditions. Each line of defense must be well designed and executed for effective implementation of the defense-in-depth concept. For example, system performance is evaluated assuming a failure of any single active component in any engineered safety feature.

In principle, defense-in-depth can be proliferated endlessly, analogous to the possible proliferation of design basis accidents. Diminishing returns from such proliferation dictate establishment of a limit to the required defense-in-depth, again analogous to the distinction between "credible" (Class 3) and "incredible" (Class 4) events. This limit, expressed as either a requirement for depth of defense or an array of credible events for which protection is required, is one of the most difficult technical safety issues to resolve. As usual, the lack of knowledge regarding probabilities is responsible for the difficulty. Judgment is rendered on an inadequate basis, and therefore is subject to change as additional knowledge is gained.

3. SOME TECHNICAL SAFETY ISSUES THAT HAVE BEEN RESOLVED

Listed in this section are examples of individual actions that have been taken on technical safety issues. Many of these actions were taken to achieve conformity or compliance with existing criteria and guides of the AEC; many were the result of decisions made on matters that arose in the context of individual cases. These examples are provided to describe the kinds of actions that have been taken, not to comment on or analyze the bases for taking such actions.

---

[1] See, for example, BECK, C.K., Role of the United States Atomic Energy Commission in control and licensing of nuclear power reactors, Nucl. Engng (Nov. 1970).

3.1 Site and Environmental Matters

Design specifications for facility structures and equipment to accommodate higher earthquake acceleration values than originally proposed have been required in many instances.

Design modifications to provide higher flood protection levels (including hurricane, storm surge, seiche and tsunami protection), than originally proposed have been required in many instances.

Protection of vital structures and equipment against tornadoes is required. The design bases for spent fuel pools have been modified in a number of cases to protect against loss of water, from pool damage, and release of fission products from fuel damage as a result of missiles propelled by tornadic winds.

For one plant site located near an airport, design modifications were required to protect against impact and fire effects of aircraft crashes.

Vent stacks have been required to be located away from containment buildings to avoid damage from a falling stack where the stacks were not designed to withstand tornadic winds.

Installation of strong motion seismographs is now a requirement for all plants.

Extensive soil and rock drilling programs have in some cases shown the need for remedial action for solution cavities, for relocation or redesign of structures, or for replacement and compaction of soil to provide suitable foundation conditions.

Design changes, such as relocation of equipment, have been required to accommodate the effects of the failure of upstream dams.

Instrumentation on towers has been required onsite to obtain local meteorological data to support adequately the assumptions made for atmospheric dispersion of radioactivity.

Environmental monitoring programs have been required to be augmented.

3.2 Reactor Design

Part-length control rods and revised instrumentation were provided to assure the capability for observing and controlling the potential effects of xenon oscillations and other power distribution anomalies.

Fixed reactivity shims were provided in the reactor core to reduce the initial value of the moderator coefficient of reactivity from a positive value to zero, so as to reduce the reactivity that would be inserted during a loss-of-coolant accident with the positive coefficient.

The capability to include fixed, incore flux detectors has been required where this capability did not exist originally.

Vibration test programs currently are required during initial cold and hot testing at the startup phase to assure acceptable performance of reactor internals and to monitor for loose parts.

3.3 Reactor Coolant System Design and Performance

Additional pipe hangers were installed as a result of a revised dynamic analysis of system piping.

Design of main steam lines was required to include a simplified dynamic analysis and improved quality control on field welds.

Stress analysis and inspection of primary coolant pump flywheels during fabrication and the capability for inspection during the service life of the flywheels is now required for all plants.

Flow restrictions have been required in main steam lines to reduce the reactivity transient following a postulated steam line break.

Material samples for monitoring the integrity of sensitized stainless steel within the primary coolant system have been required.

The design bases for reactor internals inside the reactor vessel were modified to include an allowance for blowdown forces following a loss-of-coolant accident.

The sensitivity and reliability of detection of coolant leaking from the primary system and from emergency systems were required to be improved.

Additional pipe restraints and inservice inspection have been required in the vicinity of steam generators to reduce the probability of a primary system pipe break causing a steam generator failure.

Additional restraints have been required on primary system piping to prevent the possibility of pipe whip, following a break, rupturing the containment boundary or causing other piping failures.

Replacement, or other measures to minimize the potential for cracking of furnace-sensitized stainless steel have been required in several plants.

3.4 Containment and Structures

Diagonal reinforcement for the primary containment building was required, to accommodate seismic shear forces.

Aluminum components used inside the containment building were replaced to the extent possible with steel to minimize the amount of hydrogen that might be generated from corrosion of the aluminum by the chemical solution of the containment spray system.

Improved containment building penetration design details, including leak testing ability, were required for a number of plants.

Additional protection of fuel storage pools is being required to protect against the consequences of dropping a shipping cask into the pool.

Control room shielding was required to be increased in thickness to allow normal occupancy following a postulated loss-of-coolant accident.

A fresh water storage tank was relocated since failure at its original location could have caused the failure of two diesel generators.

The intake channel and intake structure for the condenser cooling water were modified to withstand the design basis earthquake and to provide emergency cooling at minimum water level.

A containment building design was modified so that containment prestressing cable anchors would be easily accessible for inspection during operation.

All portions of the post-accident decay heat removal systems are being required to be designed to seismic Class 1 specifications.

The gaseous waste storage tanks are being required to be designed to seismic Class 1 specifications.

The response spectrum for seismic design was required to be revised to provide a more conservative design.

The design of fuel storage building was required to be revised to include provisions for controlling leakage of gaseous activity and for charcoal filtration of gaseous effluent.

Provisions are now required to deal, without the necessity of venting, with potential combustible gas mixtures generated, following a loss-of-coolant accident, by metal-water reactions in the core, radiolysis of emergency core coolant, and corrosion in the containment.

3.5 Engineered Safety Features

The designs of emergency core cooling systems and vital heat removal systems have been required to be revised to increase reliability and margin and to meet active and passive failure criteria.

Emergency Core Cooling System pump motors were required to be protected against the spray of the containment cooling system.

Chemical sprays or filters (charcoal and particulate) are being required to reduce iodine inventory after a loss-of-coolant accident to meet reduction factors required by conservative assumptions on fission product releases and meteorology.

Redundant diesel generators have been required in a number of cases to achieve adequate reliability of onsite power systems.

Rooms housing critical emergency core cooling components have been required to be sealed or separated to prevent flooding of all equipment as a result of a single failure.

Tests of vital equipment have been required under conditions simulating those attending an accident.

Filters were required to be added to the auxiliary building ventilation systems for a number of plants to mitigate the effects of a fuel handling accident.

The design was modified in a number of cases to include automatic isolation of the main condenser mechanical vacuum pump and gland seal exhausters to reduce potential doses from a rod-drop accident.

The amount of fuel for emergency diesel generators stored onsite is required to be sufficient to allow operation of engineered safety features for one week.

The containment air cooler design was required to be modified to allow detection and isolation of failure of the service water coolant lines.

Radiation detectors were required to be placed adjacent to the spent fuel pool to provide quicker detection of fission product release and resultant isolation of the reactor building in the event of leakage.

The control room ventilation system was required to close automatically on detection of radioactivity in inlet air.

Electrical heat tracing was required to be provided on the standby liquid poison control injection line (boron solution).

Physical separation and redundancy of standby gas treatment systems were required.

More conservative limits were required on the stresses, strains and deformations permitted in Class 1 systems, structures and components under seismic and accident conditions in a number of plants.

Additional equipment has been required to reduce the activity level in off-gas releases.

The design leakage rate for several containment buildings was required to be reduced.

Installation of independent overspeed protection for the turbine generator has been required for several plants.

3.6 Instrumentation and Power Systems

Changes have been required in a number of plants to achieve separation of cables servicing redundant control and protection instrumentation.

Changes have been required to improve the testability of vital instrumentation.

Switching of equipment loads between emergency diesel generators was changed from automatic to manual.

Incorporation of the split bus arrangement for emergency power supply has been required for a number of plants, resulting in the addition of another diesel generator and redesign of distribution systems.

Circuitry for a flow-biased, flux scram was required to be installed and to meet protection system standards for a number of reactor plants.

The circuitry for the rod block monitor system and auto-relief system were required to meet protection system standards for several reactor plants.

The control rod position readout system was required to be modified to give indication when rods are off their demanded position.

Instrumentation is now required to meet seismic design standards in all plants.

A redundant station battery was required.

The ability to perform a hot shutdown and the potential capability to perform a cold shutdown from outside the control room is currently required.

Diverse signals are required for actuation of the emergency core cooling systems.

Means for direct measurement of primary system coolant flow rate were required.

An alternate circuit to provide offsite power to the emergency buses was required to cope with postulated failure of the startup transformer of several plants.

Actuation instruments for engineered safety features are required to meet protection system standards.

Control systems for emergency power were required to be redesigned to meet protection system standards.

3.7 Miscellaneous

Improved development of Quality Assurance procedures and organization changes to implement these quality assurance programs have been required in many cases.

Design changes have been required in radwaste systems to reduce normal operational releases.

Redesign of fire protection systems has been required so that failure of seismic Class 2 portions of the systems will not prevent the functioning of seismic Class 1 equipment.

Interlocks and procedural restrictions have been required with respect to the crane which hoists to minimize the potential for cask drop which could damage fuel or the fuel pool.

Post-operational integrated leak rate and strength tests of the containment building are required.

Changes have been required in the operating organizations for a number of plants to include an additional supervisor and the number of licensed operators.

4. SOME TECHNICAL SAFETY ISSUES THAT HAVE NOT BEEN RESOLVED

Some examples of technical issues that are not resolved are discussed in this section. Adequate assurance of safety does not require complete resolution of these matters (see Section 1.) provided approximate conservative assumptions and procedures are used in areas where knowledge is limited.

4.1 Thermal Shock from Emergency Core Cooling

As an example of an "unresolved" technical safety issue, consider the consequences of injection of emergency core cooling water into the reactor vessel. The reactor vessel, initially at 300°C, is sprayed or flooded with cooling water initially at 25°C. The resulting thermal stress in the vessel wall can be calculated; it is not difficult to show that a perfect vessel will not be damaged. But real vessels are imperfect in at least two ways: (a) flaws smaller than some acceptance limit remain after manufacture and inspection; and (b) the properties of the material change during life because of the neutron irradiation. Therefore, the stress calculation must be performed with some conservatively hypothesized flaw present in an embrittled steel.

The only way such calculations can be made presently is ultra-conservatively, since the fracture toughness properties of thick (15-25 cm) sections of irradiated steel are not well known. These over-conservative predictions show that following long irradiation such an event might cause the vessel to crack severely. A large-scale program is underway to develop both the analytical tools and the experimental information needed to reduce the conservatism now required, but several years must elapse before this information will be available.

Today's vessels are not highly irradiated, because today's large reactors are young. So, one can put off the determination of whether something must be done about thermal shock until the information is available. If the present conjecture is disproved, and remedial measures become needed, the vessels can be annealed in place as their neutron doses reach the point where this is indicated.

Thus this problem has -- and needs-- no definitive solution for some time to come, and an appropriate program is underway to resolve the issue when needed.

4.2 Power and Peaking Limits

Another technical issue, that will never be "finally" resolved, relates to the power rating of a reactor core. The early reactors were rated very conservatively. After experience had been gained at these levels, development programs were undertaken to show, theoretically and experimentally, that higher ratings were justified. In many cases, the increased power and power density, as compared with those of previously approved reactors, have been justified on the basis that the safety margins previously evaluated have been found to be larger than originally believed. This reevaluation is usually based on measurements in the newer operating reactors, or more sophisticated calculational techniques, or the data from the development program -- in some cases on all of these things. In many instances, the new information and techniques do indeed show that the improved performance leaves margins not significantly different from those formerly thought to exist. However, it is also undeniably true that the actual safety margin will have been diminished by the uprating.

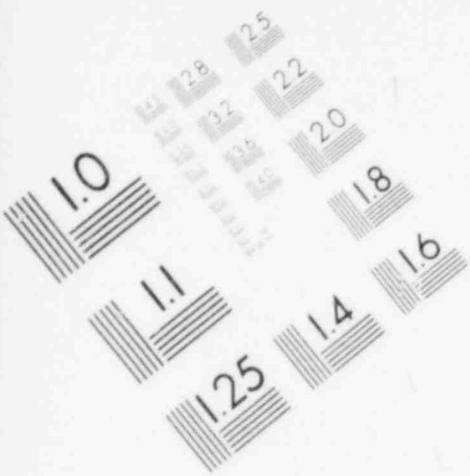
If the power increase is justified by leaving the peak power density unchanged, but running the rest of the core at higher power density (improved flattening), then the issue is rather different. The hottest part of the core is demonstrably no hotter than before. The rest of the core, though hotter than before, is still cooler -- has a greater safety margin -- than the hot spot. But any accident involving overheating will involve a larger portion of the new core than the old one, because a greater fraction of the new core runs hotter, even though the hot spot does not.

What is an appropriate limit for this procedure? Economy dictates that the core heat generation should be as nearly uniform as practical, so long as the result is safe. So far, power distributions are not so flat as to give serious concern, but a limit of flattening has not been determined. Further study is needed on the flattening question so that development of higher rated, more economical cores will not be inhibited by lack of knowledge of this safety issue.

4.3 Common-Mode Failures in Protective Systems

Protective systems and engineered safety features are composed of redundant components, arranged so that no single failure will result in system failure. Yet, when the system failures that do occur are studied, it is discovered that the majority of such events involve multiple failures, for which the probability is calculated to be very low. The actual failures are found to involve not the concurrent independent component failures usually considered in probability calculations, but causally related failures from design error, exposure to hostile environment, or human error. These common-mode, or systematic, failures are distinguished from the random failures usually considered.

Redundancy offers little defense against common-mode failures. The only technique presently known to reduce their probability of occurrence is diversity; i.e., the ability to perform the function in different ways. For the reactor protection system, diversity can be applied by monitoring different process variables



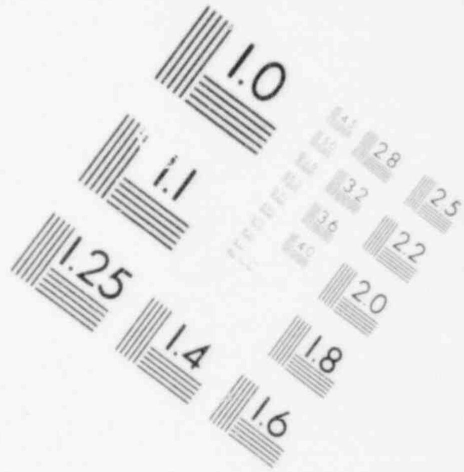
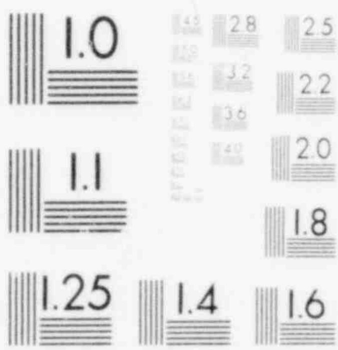
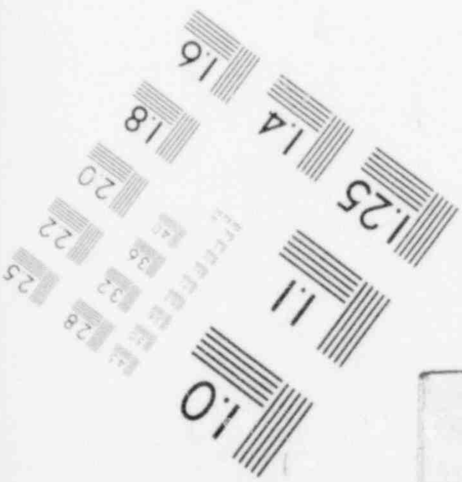


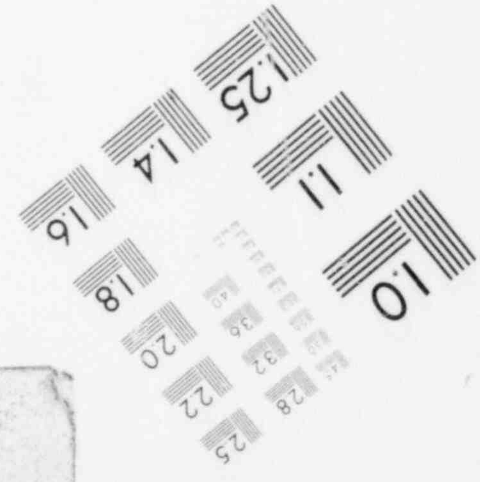
IMAGE EVALUATION TEST TARGET (MT-3)



6''

MICROCOPY RESOLUTION TEST CHART





to detect a given condition (signal diversity), by using different types of equipment to perform the same function (equipment diversity), and by employing different modes of corrective action (actuator diversity).

The study of these problems is in its infancy. A few incidents have been analyzed; a few protection systems have been studied systematically to identify potential common-mode failures; a few examples of signal diversity have been designed. The amount of improvement in reliability attainable by the use of diversity is not known, since no systems are yet known to have been designed in the United States with the full deliberate application of the three types of diversity. Moreover, the amount of improvement required, if any, is not known because the reliability of present systems is not known.

The controlling factor in requirements for protection-system reliability is the need for protection against certain anticipated operational occurrences. Examples of such occurrences are turbine trip for the boiling-water reactor and loss of power to the main circulating pumps for the pressurized water reactor. Since such events are expected to occur with a frequency of approximately once every few years, any events in this class for which failure of protective action would have unacceptable consequences will require a very high protection-system reliability in order to keep acceptably low the probability of an unprotected accident.

Study is continuing on both the probabilities of the various failures and occurrences and on their potential consequences.

4.4 Probability of Environmental Events

One of the design criteria for safety of a power reactor is that it be able to withstand the most severe earthquake, hurricane, flood or tornado that reasonably can be postulated. Clearly, each site must be evaluated in these regards. The difficulty in establishing the criteria for a specific site occurs because the recurrence interval of such severe events is very large -- thousands of years or longer. In the United States, this is longer than any historical record, and the nonhistorical record is often hard to read. The criteria for a given site therefore must be based on the best judgment of experts in seismology, meteorology, and so forth, based on frequency-severity theories necessarily unchecked in the region of concern. The result is that occasionally a site must be re-evaluated in the light of new information and the criteria revised (-- always upward, it seems. In the present state of knowledge, this appears to be unavoidable).

4.5 Performance of Emergency Core Cooling Systems

The loss-of-coolant accident (LOCA) is a Class 3 postulated improbable accident (see Section 2.3); the emergency core cooling system (ECCS) is one of the engineered safety features installed to mitigate its consequences.

The ECCS is required to be designed to do the following: (a) to limit the peak fuel cladding temperature to a safe value, currently taken to be 1260°C, (b) to limit the chemical reaction between the cladding and water to involve less than 1% of the total amount of cladding, (c) to terminate the temperature transient of the cladding so that the core geometry permits adequate cooling and before the cladding is so embrittled as to fail upon quenching, and (d) to reduce the core temperature and remove decay heat for an extended period of time.

As a result of an extensive review in 1966, programs were initiated by the Atomic Energy Commission and the nuclear industry leading to improvement in primary system integrity, development of improved analytical methods for predicting ECCS performance, and acquisition of experimental information to support and confirm the analyses.

The experimental and analytical programs are described in a companion paper.[2] The related processes of development of analytical tools and confirmatory experimentation are expected to continue. However, use of the new, more sophisticated, analysis techniques for evaluation of ECCS performance in reactor systems has begun. In view of the large amount of new information available, the Atomic Energy Commission again conducted, in 1971, a review of the current state of ECCS technology.

Ideally, one would have available analysis methods capable of detailed realistic prediction of all phenomena known or suspected to occur during a LOCA, supported in every aspect by definitive experiments directly applicable to the LOCA. In the absence of such perfection, adequate assurance of safety is obtained from an appropriately conservative analysis based on available experimental information. In areas of incomplete knowledge, conservative assumptions or procedures are applied. As further experimental information or improved calculational techniques become available, the conservatisms previously imposed can be reevaluated and a more realistic approach taken, justified by the improvement in knowledge.

The result of the 1971 review was the development of interim evaluation models consisting of computer codes, each together with its set of suitably conservative assumptions and procedures, to be applied to each plant.

[2] BROCKETT, G.F. et al., these Proceedings, Paper 39, Vol.3.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

APR 6 1979

Paile 1.7
417
Exhibit 1045

NOTE TO: Attached List

FROM: S. H. Hanauer, Assistant Director for Plant Systems, DSS

SUBJECT: 1. ENVIRONMENTAL QUALIFICATION
2. INSTRUMENTATION TO FOLLOW THE COURSE OF AN ACCIDENT

I believe that as a result of the TMI accident, we have to rethink:

1. Environmental Qualification envelope
2. Things which have to be qualified
3. RG 1.97 implementation
4. Backfitting

Changes in my thinking include:

1. Core damage is credible
2. Long-term plant operation is essential; initiation isn't enough
3. LOCA and SLB may not give an envelope that includes the TMI experience
4. We are relying heavily on things not defined as "safety-related" (Browns Ferry was like that, also)

I believe that we will be required, justifiably, to hasten the pace of review and backfitting decisions. We can't be definitely quantitative until we have better data than now available (for example, dose rates), but we can start thinking in principle.

Please start thinking about this problem. I will set a due date for your ideas as soon as we get off the night shift.

S. H. Hanauer, Assistant Director
for Plant Systems
Division of Systems Safety

cc: G. Arlotto
R. Boyd
R. DeYoung
R. Mattson
D. Ross
J. Sniezek
V. Stello

7907020144

APR 6 1979

Addressees

V. Benaroya
E. Butcher
W. Butler
A. Hintze
W. Houston
J. Knox
G. Lainas
C. Miller
T. Novak
F. Rosa
R. Satterfield
M. Srinivasan
D. Sullivan
A. Szukiewicz
R. Tedesco
D. Tondi
R. Vollmer

Fred Hebdon
AF-4E2
[illegible]
SD

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

JUL 12 1979

Exhibit 1046

MEMORANDUM FOR: Robert B. Minogue, Director
Office of Standards Development

FROM: Harold R. Denton, Director
Office of Nuclear Reactor Regulation

SUBJECT: INSTRUMENTATION TO ASSESS NUCLEAR POWER PLANT CONDITIONS DURING AND FOLLOWING AN ACCIDENT

One of the major lessons learned from the Three Mile Island accident is that better information needs to be provided to nuclear power plant operators to enable them to reliably assess what is taking place in the plant during an accident or transient situation so that they are better able to take remedial action. In addition to providing specific recommendations on instrumentation that should be required of licensees in the short term, the TMI Lessons Learned Task Force has strongly recommended that Regulatory Guide 1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident, be revised on an expedited basis for early implementation. The purpose of this revision would be to incorporate the instruments already required by the Lessons Learned Task Force plus instruments that are determined to be necessary based on a more in-depth reanalysis of the past history of Regulatory Guide 1.97 in view of the experience of the TMI-2 accident. One important criterion that should guide the revision is the need to implement, as soon as practical, state of the art equipment in operating nuclear power plants to significantly increase the ability to follow the course of an accident. Long term instrument development matters should be deferred for further study pending results from longer term investigations and decisions flowing from TMI. We believe that a minimum set of basic instrumentation to follow an accident should be required of plants now in operation as well as those under construction on an expedited basis as soon as such a list is available.

During a meeting on July 3, 1979, between representatives from my office and your office, a course of action was discussed to accomplish an expeditious review and revision of Regulatory Guide 1.97. In accordance with the discussions during that meeting, I request that SD take the lead in this effort as follows:

a. An in-depth review of instrumentation needed to assess plant conditions during and following an accident should lead to a revision to R.G. 1.97 on an expedited basis; approximately two months to establish revised positions for review by the Regulatory Requirements Review Committee.

b. Interest in providing assistance in this effort has been expressed by representatives of the national concensus standards committees and the Atomic Industrial Forum. Such assistance should be encouraged.

c. Ed Wenzinger, Chief, Reactor Systems Standards Branch, SD, will be in charge of this effort. In addition, SD will provide an engineer knowledgeable in the area of radiological monitoring.

d. NRR will assign Victor Benaroya of DSS and Leonard Soffer of DSE to assist in this effort.

If there is any problem in carrying out this effort, please let me know.

Harold R. Denton

Harold R. Denton, Director
Office of Nuclear Reactor Regulation

cc: S. Levine
V. Stello
L. Gossick

~~(Legal)~~ Distribute

EXHIBIT 1047

COMMENTS BY

ADMIRAL H. G. RICKOVER, USN
DIRECTOR
NAVAL NUCLEAR PROPULSION PROGRAM

IN MEETING WITH MEMBERS OF

THE PRESIDENT'S COMMISSION ON THE ACCIDENT AT THREE MILE ISLAND

JULY 23, 1979

JUL 24 1979

COMMENTS BY

ADMIRAL H. G. RICKOVER, USN

IN MEETING WITH MEMBERS OF

THE PRESIDENT'S COMMISSION ON THE ACCIDENT AT THREE MILE ISLAND

JULY 23, 1979

YOU HAVE ASKED ME TO PRESENT MY VIEWS ON ASPECTS OF YOUR INVESTIGATION I BELIEVE WOULD BE HELPFUL TO YOU. THE VIEWS I EXPRESS ARE MY OWN BASED ON 60 YEARS OF GOVERNMENT SERVICE. THEY DO NOT NECESSARILY REFLECT THOSE OF MY SUPERIORS.

ON MAY 24, 1979, I TESTIFIED BEFORE THE HOUSE SUBCOMMITTEE ON ENERGY, RESEARCH, AND PRODUCTION OF THE COMMITTEE ON SCIENCE AND TECHNOLOGY REGARDING MY PERSPECTIVE ON NUCLEAR SAFETY AND THE PHILOSOPHY AND APPROACH USED IN THE NAVAL REACTORS SAFETY PROGRAM. COPIES OF MY STATEMENT FOR THAT TESTIMONY HAVE BEEN PROVIDED TO YOU. I BELIEVE THE INFORMATION IN THAT STATEMENT IS AS PERTINENT TO YOUR INQUIRY AS IT WAS TO THE CONGRESSIONAL COMMITTEE.

SINCE YOU ALREADY HAVE THAT STATEMENT, I WILL NOT REPEAT ITS CONTENTS. I WILL DISCUSS THOSE MATTERS I BELIEVE TO BE OF MOST INTEREST TO YOU.

TO PROVIDE A PROPER CONTEXT AND PERSPECTIVE, HOWEVER, I WILL INCLUDE AS I PROCEED BRIEF REMARKS ON SOME OF THE MAIN POINTS I MADE THERE.

NAVAL REACTORS PROGRAM

I WILL BEGIN BY BRIEFLY DESCRIBING THE EXTENT OF THE NAVAL REACTORS PROGRAM AND OUR EXPERIENCE TO DATE: THERE ARE 127 NAVAL NUCLEAR POWERED SHIPS IN OPERATION. INCLUDING NUCLEAR SHIPS AND THE NAVAL PROTOTYPE REACTORS, I AM RESPONSIBLE FOR THE OPERATION OF 152 NAVAL REACTORS.

SINCE THE USS NAUTILUS FIRST PUT TO SEA IN 1955, NAVAL NUCLEAR POWERED SHIPS HAVE STEAMED OVER 40 MILLION MILES AND HAVE ACCUMULATED OVER 1,800 REACTOR-YEARS OF OPERATION. THIS IS SEVERAL TIMES THE APPROXIMATELY 400 REACTOR YEARS OF COMMERCIAL REACTOR OPERATION IN THE U. S. WE HAVE PROCURED 508 NUCLEAR CORES, AND HAVE PERFORMED 166 REFUELINGS.

ENVIRONMENTAL RECORD

IN THE TWENTY-SIX YEARS SINCE THE NAUTILUS LAND PROTOTYPE FIRST OPERATED THERE HAS NOT BEEN AN ACCIDENT INVOLVING A NAVAL REACTOR NOR HAS THERE BEEN ANY RELEASE OF RADIOACTIVITY WHICH HAS HAD A SIGNIFICANT EFFECT ON THE ENVIRONMENT. FOR EXAMPLE, IN EACH OF THE PAST EIGHT YEARS, THE TOTAL GAMMA RADIOACTIVITY, LESS TRITIUM, DISCHARGED IN LIQUIDS WITHIN 12 MILES OF SHORE FROM ALL OUR NUCLEAR POWERED SHIPS, SUPPORTING TENDERS, NAVAL BASES, AND SHIPYARDS, WAS LESS THAN TWO THOUSANDTHS OF A CURIE. IF ONE PERSON WERE ABLE TO INGEST THE ENTIRE AMOUNT OF THIS RADIOACTIVITY DISCHARGED FROM THE NAVAL NUCLEAR PROPULSION PROGRAM INTO ANY HARBOR IN 1978, HE WOULD NOT EXCEED THE ANNUAL RADIATION EXPOSURE PERMITTED BY THE NUCLEAR REGULATORY COMMISSION FOR AN INDIVIDUAL WORKER.

EACH YEAR I ISSUE A REPORT WHICH DESCRIBES IN DETAIL THE AMOUNT OF RADIOACTIVITY DISCHARGED TO THE ENVIRONMENT FROM OUR NAVAL SHIP OPERATIONS. THE REPORT ALSO DESCRIBES OUR METHODS OF CONTROL AND ENVIRONMENTAL MONITORING. YOU HAVE ALREADY BEEN PROVIDED WITH COPIES OF THAT REPORT.

OCCUPATIONAL RADIATION EXPOSURE

FOR THE PAST TWO YEARS THERE HAS BEEN INCREASED PUBLIC AND CONGRESSIONAL INTEREST IN THE HEALTH EFFECTS DUE TO LOW LEVEL RADIATION. MY MAY 24TH STATEMENT TO CONGRESS PROVIDED TO YOU INCLUDES A REPORT WHICH GIVES THE OCCUPATIONAL RADIATION EXPOSURE RECORD FOR CIVILIAN AND MILITARY PEOPLE INVOLVED IN THE NAVY NUCLEAR PROPULSION PROGRAM. PAGE 2 OF THAT REPORT IS A GRAPH SHOWING THE TOTAL OCCUPATIONAL RADIATION EXPOSURE TO THE PERSONNEL WHO OPERATE OUR NUCLEAR SHIPS AND TO THE WORKERS IN THE SHIPYARDS WHICH BUILD AND MAINTAIN NAVAL NUCLEAR SHIPS. IN 1978 THE TOTAL EXPOSURE WAS ABOUT ONE QUARTER THE AMOUNT IN THE PEAK YEAR 1966, EVEN THOUGH THE NUMBER OF NUCLEAR POWERED SHIPS OPERATING IN 1978 WAS NEARLY DOUBLE THAT IN 1966. THIS REDUCTION IN OCCUPATIONAL EXPOSURE DID NOT JUST HAPPEN. IT REQUIRED HARD WORK AND CONSTANT ATTENTION BY EVERYONE - WORKERS AND MANAGEMENT.

THE REPORT SHOWS THAT SINCE 1967 NO CIVILIAN OR MILITARY PERSONNEL IN THE NAVY'S NUCLEAR PROPULSION PROGRAM HAVE EXCEEDED THE QUARTERLY FEDERAL LIMIT OF 3 REM OR ANNUAL RADIATION

EXPOSURE LIMIT OF 5 REM. THE AVERAGE ANNUAL JOB-RELATED EXPOSURE OF SHIPYARD RADIATION WORKERS IN 1978 WAS ONE QUARTER OF A REM. THE AVERAGE ANNUAL JOB-RELATED EXPOSURE OF NUCLEAR SHIP PROPULSION PLANT OPERATORS IN 1978 WAS ONE TENTH OF A REM. THE REPORT ALSO OUTLINES MANY OF THE MEASURES EMPLOYED TO LIMIT OCCUPATIONAL RADIATION EXPOSURE.

I BELIEVE .AT THE REPORTS ON RADIOACTIVE DISCHARGE AND ON RADIATION EXPOSURE WILL BE OF VALUE TO YOU BECAUSE THEY CONVEY SOME IDEA OF THE HARD WORK AND ATTENTION TO DETAIL WHICH WE HAVE APPLIED TO MAINTAIN HIGH ASSURANCE THAT THE PUBLIC AND THOSE IN THE NAVAL PROGRAM ARE PROTECTED.

DIFFERENCES BETWEEN NAVAL REACTOR AND COMMERCIAL NUCLEAR PLANTS

SINCE THE THREE MILE ISLAND INCIDENT, THERE HAS BEEN INCREASED INTEREST IN COMPARING COMMERCIAL AND NAVAL REACTOR PLANTS. USEFUL LESSONS CAN BE LEARNED FROM THIS. BUT I MUST CAUTION AGAINST ANY ATTEMPT TO APPLY DIRECTLY TO COMMERCIAL PLANTS ANY SPECIFIC FEATURES, METHODS OR PROCEDURES FROM NAVAL REACTORS - OR TO APPLY DIRECTLY TO NAVAL APPLICATIONS ANY SPECIFICS FROM COMMERCIAL NUCLEAR REACTORS.

THERE ARE FUNDAMENTAL DIFFERENCES BETWEEN NAVAL AND CIVILIAN NUCLEAR POWER PLANTS BECAUSE OF SPECIFIC MILITARY

REQUIREMENTS WHICH MUST BE MET BY NAVAL PROPULSION REACTORS. MANY OF THESE ARE, OF NECESSITY, MORE EXACTING THAN THOSE FOR CENTRAL STATION PLANTS. FOR EXAMPLE, THE SHOCK LOADINGS DUE TO UNDERWATER EXPLOSIONS, FOR WHICH NAVAL PLANTS ARE DESIGNED, ARE FAR GREATER THAN THE EARTHQUAKE SHOCK LOADINGS FOR WHICH CIVIL' PLANTS ARE DESIGNED. IN ADDITION, BECAUSE MANEUVERABILITY IS ESSENTIAL FOR MILITARY SHIPS, NAVAL PLANTS ARE DESIGNED TO ACCOMMODATE MUCH MORE RAPID AND FREQUENT POWER TRANSIENTS THAN THOSE EXPERIENCED IN CIVILIAN PLANTS. ALSO, EACH NAVAL SHIP MUST DEPEND ENTIRELY ON ITS OWN POWER PLANT. THERE IS NO INTERCONNECTED GRID TO PICK UP THE LOAD TO ALLOW THE SHIP TO CONTINUE FUNCTIONING.

BECAUSE OUR SHIPS MUST BE ABLE TO OPERATE AT SEA UNDER COMBAT CONDITIONS WE INSIST ON CONSERVATISM IN EVERY ELEMENT OF NAVAL REACTOR PLANTS. CENTRAL STATION PLANTS ARE DESIGNED TO PROVIDE RELIABLE POWER AT MINIMUM COST. THESE DIFFERENT OBJECTIVES ARE REFLECTED IN ELEMENTS OF THESE PLANTS.

COMPARISONS AND CONCLUSIONS MUST TAKE THESE DIFFERENCES INTO ACCOUNT.

NEED TO AVOID OVER-CONCENTRATION ON SPECIFICS

I AM NOT AN EXPERT ON THE THREE MILE ISLAND INCIDENT. OTHERS ARE FAR MORE KNOWLEDGEABLE OF THE DETAILS OF THAT PLANT DESIGN AND THE EVENTS LEADING TO THE INCIDENT. YOU AND YOUR

STAFF AS WELL AS SEVERAL OTHER GROUPS ARE DEVOTING CONSIDERABLE TIME TO UNDERSTANDING IT. THEREFORE, I WILL NOT ATTEMPT TO COMMENT ON THE TECHNICAL DETAILS OF THE PLANT OR THE EVENT.

FURTHER, THERE IS A DANGER THAT OVER-CONCENTRATION ON THE DETAILS OF THIS ONE INCIDENT WILL HINDER IDENTIFICATION OF STEPS WHICH MIGHT PROVIDE GREATER OVERALL ASSURANCE OF THE SAFETY OF COMMERCIAL NUCLEAR POWER. I WILL THEREFORE CONCENTRATE ON PRINCIPLES RATHER THAN ON DETAILED FEATURES OR COMPARISONS.

BASIC PRINCIPLES OF NAVAL REACTORS PROGRAM

OVER THE YEARS, I HAVE FREQUENTLY BEEN ASKED HOW I RUN THE NAVAL REACTORS PROGRAM. SOME BELIEVE I HAVE A SIMPLE, EASY GIMMICK THAT MAKES MY PROGRAM FUNCTION. THEY ARE DISAPPOINTED TO FIND THERE IS NONE - THE SUCCESS OF ANY PROGRAM DEPENDS ON MANY INTERRELATED FACTORS.

THIS THOUGHT IS IMPORTANT IN YOUR DELIBERATIONS. THE PROBLEMS YOU ARE INVESTIGATING CANNOT BE SOLVED BY DIRECTING COMPLIANCE WITH ONE OR TWO SIMPLE PROCEDURES. REACTOR SAFETY REQUIRES ADHERENCE TO A TOTAL CONCEPT WHEREIN ALL ELEMENTS ARE RECOGNIZED AS IMPORTANT AND EACH IS CONSTANTLY REINFORCED.

I WILL DISCUSS SOME OF THE PRINCIPLES I BELIEVE WILL BE OF INTEREST TO YOU. OTHERS WERE DISCUSSED IN DETAIL IN MY PRIOR TESTIMONY TO WHICH I HAVE REFERRED, AND WHICH YOU HAVE.

STRONG CENTRAL TECHNICAL CONTROL

ALL ASPECTS OF NAVAL NUCLEAR PROPULSION ARE CONTROLLED BY ONE CENTRAL TECHNICAL ORGANIZATION. IT IS NOT POSSIBLE TO SEPARATE THE RESPONSIBILITY AND AUTHORITY INTO SEPARATE PHASES OR PACKAGES WITH EACH ASSIGNED TO AN INDEPENDENT GROUP. DESIGN, MANUFACTURE, ASSEMBLY, TEST, OPERATION, MAINTENANCE AND SELECTION AND TRAINING OF PERSONNEL ARE SO CLOSELY INTERRELATED AS TO REQUIRE CLOSE TECHNICAL COORDINATION AND DIRECTION. A TECHNICALLY COMPETENT HEADQUARTERS STAFF AND EXPLICIT PROVISIONS TO HAVE PROBLEMS BROUGHT DIRECTLY TO THE ATTENTION OF TOP MANAGEMENT ARE ESSENTIAL. FOR EXAMPLE, I GET FREQUENT REPORTS OF PROBLEMS - NOT THE GOOD NEWS BUT THE BAD NEWS - FROM EACH OF OUR LABORATORIES, MAJOR MANUFACTURERS, SHIPS, AND SHIPYARDS.

I ALSO SEE THAT OUR DESIGNERS KNOW WHAT THEY ARE WORKING ON; THEY SEE COMPONENTS BEING BUILT AND PLANTS BEING CONSTRUCTED AND OPERATED.

TECHNICAL COMPETENCE

IN A COMPLEX TECHNICAL AREA SUCH AS NUCLEAR POWER, ALL INDIVIDUALS WHO MAKE DECISIONS IN ACQUISITION, DESIGN, OPERATION, MAINTENANCE TRAINING, ETC., MUST UNDERSTAND THE TECHNOLOGY INVOLVED. THEY MUST HAVE A FUNDAMENTAL UNDERSTANDING OF AND COMMITMENT TO THE TECHNICAL ASPECTS OF THE JOB AND A DETERMINATION TO SEE THAT CAREFUL ATTENTION IS PAID TO THE TECHNICAL DETAILS.

IN DISCUSSING TRAINING IN THE NUCLEAR BUSINESS MOST PEOPLE THINK OF THE PLANT OPERATORS - MOST OF THE DISCUSSION I HAVE HEARD HAS CONCERNED ITSELF WITH JUST THAT - TRAINING OF OPERATORS. NUCLEAR POWER, HOWEVER, REQUIRES A MORE BASIC AND BROADER CONCEPT OF TRAINING. LIKE ALL NEW TECHNOLOGIES, IT ESTABLISHES ITS OWN REQUIREMENTS. EVERYONE INVOLVED MUST UNDERSTAND AND APPRECIATE THE TECHNICAL ASPECTS OF NUCLEAR POWER AND HAVE A DEEP SENSE OF RESPONSIBILITY AND A DEDICATION TO EXCELLENCE. THIS INCLUDES THE UTILITY MANAGERS, THE PLANT DESIGNERS, THE COMPONENT DESIGNERS AND FABRICATORS, THE ARCHITECT ENGINEERS, THE CONSTRUCTION COMPANIES - PARTICULARLY THEIR INSPECTORS, THE ENGINEERS AND TECHNICIANS WHO ASSEMBLE AND TEST THE PLANT, THE PEOPLE WHO MAINTAIN AND CALIBRATE THE EQUIPMENT, THE OPERATORS, ETC.

WHEN I STARTED THE NAVAL NUCLEAR PROGRAM I DEVOTED MYSELF TO THE TRAINING OF MANAGEMENT AND KEY PERSONNEL IN ALL THE ORGANIZATIONS INVOLVED AND TO SEEING THAT THEY IN TURN TRAINED THE REST OF THEIR PEOPLE. THIS IS STILL A MAJOR ELEMENT OF THE NAVAL REACTORS PROGRAM - SEEING THAT ALL ORGANIZATIONS INVOLVED HAVE QUALIFIED AND TRAINED PEOPLE. EACH PRIME CONTRACTOR IS REQUIRED TO HAVE A TRAINING PROGRAM FOR SUCH PEOPLE AS DESIGN ENGINEERS, FIELD REPRESENTATIVES, TECHNICAL AUDITORS, AND INSPECTORS. FURTHER, THEY ARE REQUIRED TO HAVE MANAGERS WHO KNOW WHAT THEY ARE DOING, TECHNICALLY AND WHO ARE RUNNING THE

JOB - NOT JUST REPORTING ON IT AND PASSING ON THE RECOMMENDATIONS OF SUBORDINATES. MANAGERS MUST GET OUT OF THEIR OFFICES AND SEE WHAT IS REALLY GOING ON. MY REPRESENTATIVES CHECK ON THE EFFECTIVENESS OF THESE TRAINING PROGRAMS.

WE ALSO REQUIRE THAT PERSONNEL SUCH AS PLANT TEST ENGINEERS AT OUR SHIPYARDS, AND KEY INSPECTORS AT ALL OUR VENDORS, BE QUALIFIED AND TESTED BY NAVAL REACTOR PROGRAM PERSONNEL IN ACCORDANCE WITH NAVAL REACTORS APPROVED STANDARDS. IN OTHER CASES, WE SPECIFY THE SCOPE AND EXTENT OF TRAINING NEEDED AND THEN THE COMPANY HAS TO CARRY IT OUT AND CONDUCT APPROPRIATE WRITTEN AND ORAL EXAMS OR ACTUAL DEMONSTRATIONS. IN ALL CASES, HOWEVER, STEPS ARE TAKEN TO ASSURE THAT EACH ORGANIZATION HAS ADEQUATE MEANS TO PROVIDE QUALIFIED PEOPLE, AND TO CHECK UP ON THEM.

FOR PERSONNEL AT NAVAL REACTORS HEADQUARTERS, MEMBERS OF MY SENIOR STAFF AND I PERSONALLY INTERVIEW EACH CANDIDATE TO ENSURE HE IS COMPETENT TECHNICALLY AND HAS THE RIGHT ATTITUDES AND MOTIVATION. THEY ARE THEN TRAINED IN THE DETAILS OF REACTOR PLANT DESIGN, CONSTRUCTION, AND OPERATION, AND TAUGHT TO MANAGE THE PROGRAM THROUGH A THOROUGH KNOWLEDGE OF THE TECHNICAL FACTS, LOGIC, COMMON SENSE, AND HARD WORK.

CONSERVATISM OF DESIGN

IN ANY ENGINEERING ENDEAVOR, AND PARTICULARLY IN A HIGHLY TECHNICAL FIELD SUCH AS NUCLEAR POWER, CONSERVATISM IS ESSENTIAL.

The design must, from the very beginning, allow for all the uncertainty and inaccuracy in the available knowledge. If the basic design is not conservative, it becomes necessary to compensate by adding design features or systems. These added features or systems increase the complexitity of the plant, make it harder to understand and operate, and thus reduce conservatism, reliability, and safety.

Another important concept in design is what I refer to as making the plant "sailor proof". I introduced this concept in the early days of the Naval Nuclear Program. It means that the designer must assure that the plant, its equipment and its procedures are such that the sailors who will operate the plant can be expected, realistically, to understand, operate and maintain it properly. The concept also requires that the plant be designed to accommodate, insofar as practicable, operator errors that may occur - that it be "forgiving" and that its arrangement allow ready access for needed repairs.

My May 24, 2979 statement contains many examples of conservative design practices used in the Naval Reactors Program. The following ones may be of particular interest to you:

- USE SIMPLE SYSTEM DESIGNS SO THAT RELIANCE IS PLACED PRIMARILY ON DIRECT CONTROL BY TRAINED OPERATORS RATHER THAN ON AUTOMATIC CONTROL.

- DESIGN, BUILD, OPERATE, AND MAINTAIN THE PLANT SO AS TO PREVENT ACCIDENTS, RATHER THAN RELYING ON SYSTEMS AND PROCEDURES PROVIDED TO COPE WITH ACCIDENTS AFTER THEY OCCUR.

- DESIGN THE PLANT SO THAT, AS FAR AS PRACTICABLE, ITS RESPONSE TO EXPECTED TRANSIENTS IS SELF-LIMITING AND ALLOWS REASONABLE TIME FOR THE OPERATOR TO CONTROL THE PLANT PRIOR TO REQUIRING AUTOMATIC PROTECTIVE ACTION.

- USE FORMAL DOCUMENTATION FOR ALL PARTS OF THE PROGRAM - DESIGN DECISIONS, MANUFACTURING PROCEDURES, OPERATING PROCEDURES,

INSPECTION REQUIREMENTS, INSPECTION RESULTS, AND FOR ANY WAIVERS. TECHNICAL FACTS, RECOMMENDATIONS AND DECISIONS MUST BE THOROUGHLY REVIEWED BY SENIOR PERSONNEL IN ALL THE DISCIPLINES INVOLVED. TECHNICAL ACTION BY LOCAL RESIDENTS CANNOT BE ALLOWED. THE DECISIONS AND THE BASES FOR THEM MUST BE IN WRITING AND THE DOCUMENTATION MUST BE KEPT FOR REFERENCE USE AS LONG AS THE PLANT IS IN OPERATION.

- CONDUCT FREQUENT, THOROUGH, AND DETAILED AUDITS OF ALL ASPECTS OF THE PROGRAM BY INDIVIDUALS SELECTED AND TRAINED FOR THIS PURPOSE. THERE SHOULD BE BOTH UNANNOUNCED AUDITS AND EXTENDED OBSERVATIONS OF INDIVIDUAL OPERATIONS.

COMPLIANCE WITH DETAILED OPERATING PROCEDURES

OPERATING A NUCLEAR POWER PLANT PROPERLY REQUIRES KNOWLEDGE AND UNDERSTANDING OF THE CHARACTERISTICS OF MANY SYSTEMS AND COMPONENTS, AND OF THEIR INTERACTIONS. RELIANCE MUST ULTIMATELY BE PLACED ON THE OPERATOR. HOWEVER, WE PROVIDE, INSOFAR AS PRACTICABLE, DETAILED PROCEDURES FOR THOSE OPERATIONS AND CASUALTIES WHICH CAN BE FORESEEN. PREPARING SUCH PROCEDURES ALLOWS DELIBERATE, THOROUGH CONSIDERATION BY A NUMBER OF PEOPLE OF ALL THE FACTORS INVOLVED. IT ALSO PROVIDES A LARGE DEGREE OF STANDARDIZATION AND PROVIDES A MEANS TO IMPROVE THE PROCEDURES BASED ON OPERATING EXPERIENCE. WHERE PROCEDURES ARE PROVIDED TO THE OPERATOR WE REQUIRE VERBATIM COMPLIANCE. IF THE OPERATOR

BELIEVES THE PROCEDURE TO BE WRONG OR FINDS IT CANNOT BE CARRIED OUT AS WRITTEN, HE MUST STOP AND OBTAIN APPROVAL OF A REVISED PROCEDURE. SIMILARLY, IF HE BELIEVES THE PROCEDURE CAN BE IMPROVED, HE IS TO RECOMMEND A CHANGE BUT NOT IMPLEMENT IT UNTIL IT IS APPROVED. IF NO PROCEDURE EXISTS FOR A PLANNED EVOLUTION, ONE IS TO BE WRITTEN AND APPROVED BEFORE PROCEEDING.

OF COURSE, IN A TRUE EMERGENCY THE OPERATORS MUST DO WHAT THEY JUDGE NECESSARY - BUT THE VAST MAJORITY OF SITUATIONS ARE COVERED BY APPROVED PROCEDURES. KNOWLEDGE AND UNDERSTANDING OF THEM AND THE BASES FOR THEM AID THE OPERATOR TO UNDERSTAND THE PLANT AND DECIDE WHAT TO DO WHEN HE HAS TO ACT ON HIS OWN.

DON'T "LIVE WITH" DEFICIENCIES

IT IS NAIVE TO ALLOW ROUTINE OPERATION WITH MANY DEFICIENCIES SUCH AS "ALARMS" OR ABNORMAL CONDITIONS PRESENT, AND THEN EXPECT OPERATORS TO RESPOND PROPERLY TO ALARMS WHICH INDICATE A CASUALTY. ONCE YOU LEARN TO "LIVE WITH" DEFICIENCIES SUCH AS SIGNIFICANT LEAKAGE AND A NUMBER OF ALARMS OR ABNORMAL CONDITIONS, THERE ENSUES A LOSS OF ABILITY TO RECOGNIZE AND RESPOND TO NEW PROBLEMS OR NEW CONDITIONS WHICH MAY ACTUALLY JEOPARDIZE THE PLANT BUT SEEM TO BE JUST ANOTHER ACCEPTABLE DEFICIENCY.

IT IS UNUSUAL FOR MY PLANTS TO OPERATE WITH ANY ALARMS FOR AN EXTENDED PERIOD OF TIME; EXTENDED OPERATION WITH SEVERAL ALARMS IS UNHEARD OF.

In conclusion, I believe the staff should evaluate underfrequency protection on operating plants as well as plants under review. Furthermore, the compatibility of higher frequency decay rates with low power levels should also be evaluated to ascertain the worst case conditions for plant operation.

4. Issue No. 10 - Grid Stability

The Millstone incident in my view was not a grid stability incident per se. Incidents such as these, however, can lead to loss of generation as it has in this case, which could alternately result in broad grid instability. Therefore, adequate technical specifications should be developed to require periodic testing of the emergency power systems to conditions of LOCA loadings to assure the systems' proper response.

In conclusion, I believe that operating plants as well as plants under review should develop technical specifications to require integrated ESF tests at refueling shut downs. Mini-flow conditions and/or blocked valves on pumps and fans would allow sufficient challenge on power systems to assure their proper response in starting and accelerating their motor loads. Furthermore, the staff should develop the capability to independently evaluate stability of grids that supply offsite power to nuclear plant distribution systems, (see memorandum from W. R. Butler to D. G. Eisenhut dated August 18, 1976).

5. Issue No. 12 - Load Break Switch

Load break switches are not used for the purpose described in your memorandum to the staff, Generator Breakers are the devices used for that purpose.

Clarification of the requirements needed to make these devices acceptable for use in nuclear plants has been transmitted to Dr. Heineman by memorandum dated October 26, 1976.

B. The following are my comments on allegations made, that portions of the NRC response submitted to the Joint Committee on Atomic Energy regarding allegations raised by Robert Pollard did not adequately reflect the information supplied by NRC technical reviewers (see memorandum dated November 8, 1976, from Roger Fortuna and William Foster to T. J. McTiernan, Director, Office of Inspector and Auditor):

1. Underfrequency Protection for Indian Point Units 2 and 3

My supervisor asked me to look into the underfrequency protection provided for Indian Point Units 2 and 3, and report my assessment of the adequacy of the underfrequency protection provided for this plant.

TRAINING OF PLANT OPERATORS

I CONSIDER THE SELECTION AND TRAINING OF THE OFFICERS AND ENLISTED MEN WHO OPERATE OUR SHIPS TO BE AT LEAST AS IMPORTANT TO SAFETY AS ANY OTHER ELEMENT OF THE NAVY NUCLEAR POWER PROGRAM. THE MENTAL ABILITIES, JUDGMENT, AND LEVEL OF TRAINING OF PLANT OPERATORS MUST BE COMMENSURATE WITH THE RESPONSIBILITY INHERENT IN OPERATING A NUCLEAR PLANT. SELECTION AND TRAINING OF PERSONNEL IN THE NAVAL NUCLEAR POWER PROGRAM ARE CARRIED OUT WITH THESE CONSIDERATIONS IN MIND.

ACADEMIC ABILITY, PERSONAL CHARACTER AS DEMONSTRATED BY ANY ACTS REFLECTING UNRELIABILITY, AND PERSONAL MOTIVATION ARE TAKEN INTO ACCOUNT IN SELECTION OF PERSONNEL. ONCE SELECTED, THE INDIVIDUAL IS CONTINUALLY SUBJECTED TO REVIEW. NOT ALL THOSE SELECTED FOR TRAINING PASS THE COURSE AND QUALIFY. SOME HAVE TO BE DROPPED. ALSO, IT IS NOT SUFFICIENT TO QUALIFY AN OPERATOR ONCE, AND THEN LET HIM ALONE. THEREFORE, OUR TRAINING PROGRAM IS A CONTINUING ONE. THE SAME STANDARDS ARE USED FOR REQUALIFICATION AS FOR INITIAL QUALIFICATION - AND, AGAIN, NOT EVERYONE REQUALIFIES - SOME FAIL AND ARE DROPPED.

I WANT TO MAKE CLEAR THAT WE TRAIN AND QUALIFY ALL PROPULSION PLANT OPERATORS - INCLUDING STEAM PLANT OPERATORS.

THERE IS SUCH A DIRECT INTERACTION OF THE STEAM PLANT AND THE REACTOR PLANT THAT THIS IS REQUIRED.

IN ADDITION TO THE TRAINING AND RETRAINING PROGRAMS, INSPECTIONS OF PERSONNEL IN THE FLEET ARE CONDUCTED BY MEMBERS OF MY STAFF - BOTH FROM FIELD OFFICES AND FROM HEADQUARTERS. ADDITIONAL INSPECTIONS ARE CONDUCTED BY SPECIAL EXAMINING BOARDS ESTABLISHED BY THE CHIEF OF NAVAL OPERATIONS AND BY NUCLEAR TRAINED PERSONNEL ON VARIOUS OTHER NAVAL STAFFS. I REVIEW THE RESULTS OF ALL INSPECTIONS.

I HAVE ESTABLISHED A FORMAL SYSTEM OF REPORTING PROPULSION PLANT PROBLEMS WHICH IDENTIFIES AREAS IN NEED OF IMPROVEMENT IN THE TRAINING PROGRAM. I ALSO REQUIRE THE COMMANDING OFFICER OF EACH NUCLEAR POWERED SHIP TO WRITE ME PERIODICALLY CONCERNING PROPULSION PLANT PROBLEMS. THESE LETTERS MUST ALSO CONTAIN DETAILED INFORMATION ON THE TRAINING HE HAS CONDUCTED SO I CAN EVALUATE WHETHER SUFFICIENT TIME AND ATTENTION ARE BEING PAID TO THIS IMPORTANT AREA.

ANOTHER IMPORTANT ASPECT OF OUR TRAINING PROGRAM IS OUR INSISTENCE THAT OPERATORS BELIEVE THEIR INSTRUMENTS UNLESS AND UNTIL THEY ARE PROVEN WRONG. IF THEY CONSIDER AN INSTRUMENT TO BE IN ERROR, THEY MUST REPORT IT IMMEDIATELY. OUR OPERATORS ARE DRILLED CONSTANTLY ON THIS PRINCIPLE AND TAUGHT THAT THEY CANNOT IGNORE INSTRUMENT READINGS EVEN IF THEY BELIEVE THEM TO BE

INVALID. THEY ARE ALSO DRILLED IN WHAT AN INSTRUMENT READING REALLY MEANS AND HOW IT CAN BE AFFECTED BY CASUALTY CONDITIONS. IN CASE OF DOUBT AS TO THE ACTUAL MEANING, THEY ARE SPECIFICALLY TAUGHT TO BELIEVE THE WORST.

THERE IS ONE OTHER POINT WITH REGARD TO TRAINING I WANT TO EMPHASIZE - AND IT IS THIS: TOP MANAGEMENT PERSONNEL MUST BE TECHNICALLY KNOWLEDGEABLE AND BE FULLY INVOLVED IN SEEING THAT THE TRAINING IS DONE PROPERLY. IT IS INSUFFICIENT AND MISLEADING FOR MANAGEMENT TO DEAL, AS MANY DO, SOLELY WITH THE TOTAL NUMBER OF MAN MONTHS OF TRAINING OR THE LENGTH OF THE PROGRAM, OR THE COST, OR THE FACILITIES, OR TO DELEGATE TRAINING TO A SUBCONTRACTOR, THEREBY LEAVING THE VITAL "DETAILS" TO SOMEONE ELSE.

SIMILARLY, THE CONTENT OF THE PROGRAM CANNOT BE DEVELOPED BY THE DESIGNERS ALONE OR BY OPERATORS ALONE - BOTH MUST BE DEEPLY INVOLVED ON A CONTINUING BASIS.

THESE ARE JUST THE MAIN ELEMENTS OF THE TRAINING EFFORTS IN MY PROGRAM. BECAUSE TRAINING IS SO IMPORTANT, I HAVE PROVIDED, IN MY MAY 24TH STATEMENT, A MUCH MORE DETAILED DESCRIPTION OF OUR TRAINING OF PLANT OPERATORS. I RECOMMEND THAT ALL THE COMMISSION MEMBERS AND YOUR STAFF READ IT.

SOME HAVE SUGGESTED THAT THE SUCCESS OF NAVAL NUCLEAR POWER IS A RESULT OF THE DISCIPLINE WHICH CAN BE ENFORCED IN A

MILITARY ENVIRONMENT, BUT WHICH CANNOT BE ACHIEVED IN A COMMERCIAL NUCLEAR ENVIRONMENT. I DO NOT AGREE. I BELIEVE THAT ADEQUATE DISCIPLINE CAN BE OBTAINED IN COMMERCIAL NUCLEAR POWER.

DISCIPLINE IS AN ESSENTIAL CHARACTERISTIC OF ANY SUCCESSFUL PROGRAM AND OF ANY SUCCESSFUL PERSON. THE DISCIPLINE IN THE NAVAL NUCLEAR PROGRAM HAS BEEN SUCCESSFUL, NOT BECAUSE THIS INVOLVES MILITARY APPLICATIONS, BUT BECAUSE I HAVE INSISTED UPON STAFFING THE PROGRAM WITH INTELLIGENT, MOTIVATED PEOPLE, WHOM I HOLD ACCOUNTABLE. ACHIEVING THE REQUIRED DISCIPLINE IN THE COMMERCIAL NUCLEAR FIELD WILL REQUIRE ATTENTION TO RESPONSIBILITY AND THE OTHER THINGS I HAVE SUGGESTED, AND RECOGNITION BY ALL INVOLVED THAT TAKING PART IN DESIGNING, BUILDING, AND OPERATING A NUCLEAR POWER PLANT IS NOT A "RIGHT" GIVEN TO EACH AMERICAN AT BIRTH ANY MORE THAN BEING A SURGEON OR AN AIRLINE PILOT HAS SUCH A "RIGHT". SELECTION AND RETENTION OF PEOPLE MUST BE BASED SOLELY ON COMPETENCE AND PERFORMANCE. THESE MUST NOT BE SUBORDINATED TO OTHER GOALS. MANAGEMENT RESPONSIBLE FOR SAFE OPERATION MUST HAVE THE AUTHORITY TO ENFORCE STANDARDS.

FORMALITY AND DISCIPLINE

ANOTHER IMPORTANT ASPECT OF OPERATING A NUCLEAR PLANT IS TO ENSURE THAT THE OPERATORS' ATTENTION IS CONSTANTLY FOCUSED ON THE PLANT. THIS IS DIFFICULT, PARTICULARLY IF THE PLANT IS

OPERATING AT A STEADY STATE CONDITION. IN THIS SITUATION THE OPERATOR HAS LITTLE OR NO DIRECT ACTION TO TAKE - HE MERELY MONITORS. THERE IS THEN AN INEVITABLE TENDENCY FOR HIS ATTENTION TO DRIFT - FOR IDLE CONVERSATION OR EVEN READING OR EATING TO TAKE PLACE. THIS CANNOT BE TOLERATED.

CLEAR COMMUNICATIONS ARE ESSENTIAL IN DEALING WITH NUCLEAR POWER. THERE IS NO PLACE FOR MISUNDERSTANDING OR FOR GUESSING WHAT IS MEANT. IN MOST HUMAN COMMUNICATION, PARTICULARLY AMONG THOSE WHO ARE ACCUSTOMED TO DEAL FREQUENTLY AND CLOSELY WITH ONE ANOTHER, PRECISE LANGUAGE IS OFTEN NOT USED OR REQUIRED, MUCH OF THE MEANING BEING CONVEYED BY TONE OR GESTURE.

THIS IS NOT ACCEPTABLE IN THE OPERATION OF ANY ADVANCED TECHNOLOGY SUCH AS NUCLEAR POWER. ALL COMMUNICATIONS MUST BE PRECISE, USING STANDARD TERMINOLOGY WHICH LEAVES NO MEANING TO BE IMPLIED AND REQUIRES NO INTERPRETATION. ALL ORDERS MUST BE GIVEN <u>AND ACKNOWLEDGED</u> IN SPECIFIC AUTHORIZED TERMS.

FOR FORMALITY AND DISCIPLINE TO OBTAIN WHEN THERE IS AN EMERGENCY, IT MUST HAVE BEEN PRESENT WHEN THINGS WERE GOING ROUTINELY. CREWS THAT ENGAGE IN TALK NOT DIRECTLY RELATED TO PLANT CONDITIONS OR OPERATIONS OR WHO INDULGE IN SLOPPY PERSONAL HABITS ON WATCH WILL NOT RESPOND QUICKLY AND CORRECTLY TO A FAST MOVING PROBLEM.

IN THE NAVAL PROGRAM WE PAY CAREFUL ATTENTION TO STRICT FORMALITY. WHENEVER THE PLANT IS OPERATING, THERE ARE ON DUTY NOT

JUST THE QUALIFIED OPERATORS BUT ALSO QUALIFIED OFFICERS WHO SUPERVISE THEM. ONE OF THE SUPERVISOR'S RESPONSIBILITIES IS TO ASSURE FORMALITY, DISCIPLINE, AND ATTENTION. IN CIVILIAN PLANTS, WHICH OPERATE LARGELY AT STEADY POWER CONDITIONS AND WHERE THE INDIVIDUALS ARE ON WATCH FOR EIGHT HOURS AT A TIME INSTEAD OF FOUR AS IN THE NAVY, IT IS MORE DIFFICULT TO ACHIEVE THE PROPER WATCHSTANDING PRACTICES.

MUCH TIME AND ENERGY IS REQUIRED TO ACHIEVE STRICT WATCH-STANDING PRACTICES AND TO AVOID CONFUSION IN COMMUNICATIONS. THIS IS ALWAYS NECESSARY, AND ESPECIALLY WHEN A CRISIS ARISES.

DANGER OF PLACING UNDUE RELIANCE ON PRIOR INVOLVEMENT IN NAVAL NUCLEAR PROGRAM

IT APPEARS THAT SOME IN THE CIVILIAN NUCLEAR INDUSTRY AND, PERHAPS, THE NRC HAVE BEEN PLACING UNDUE RELIANCE ON THE MERE FACT THAT A PERSON HAS BEEN INVOLVED IN THE NAVAL NUCLEAR PROGRAM.

I BELIEVE THE TRAINING PROVIDED TO OPERATORS IN THE NAVAL NUCLEAR PROGRAM IS FULLY ADEQUATE AND EQUAL TO THAT ANYWHERE. HOWEVER, SUCCESSFULLY COMPLETING A TRAINING PROGRAM IS IN ITSELF NOT ENOUGH TO QUALIFY ONE TO ESTABLISH OR RUN SUCH A PROGRAM. ALSO, AS I POINTED OUT EARLIER, OPERATOR TRAINING IS ONLY ONE ELEMENT OF THE TOTAL PROGRAM. OTHER ESSENTIAL ELEMENTS ARE STAFFING LEVELS, SUPERVISION, AUDITING AND QUALIFICATION, AND REQUALIFICATION FOR THE SPECIFIC PLANT TO BE OPERATED.

FINALLY, IT MUST BE RECOGNIZED THAT UNDER PRESENT LAWS AND REGULATIONS IT IS NOT EVEN POSSIBLE FOR A PROSPECTIVE EMPLOYER TO DETERMINE WHETHER AN INDIVIDUAL WHO WAS IN THE NAVAL NUCLEAR PROGRAM PERFORMED SATISFACTORILY OR NOT. PRIVACY REGULATIONS PREVENT THE NAVY FROM RELEASING SUCH INFORMATION UNLESS SPECIFICALLY AUTHORIZED BY THE INDIVIDUAL.

THERE ARE AND HAVE BEEN MANY COMPETENT HIGHLY TRAINED PEOPLE IN THE NAVAL NUCLEAR PROGRAM - BUT THE RESPONSIBILITY TO EVALUATE THEIR COMPETENCE AND PERFORMANCE WITH RESPECT TO ANY

JOB IN CIVILIAN NUCLEAR POWER RESTS WITH THEIR CIVILIAN EMPLOYERS - WHO ALSO HAVE THE RESPONSIBILITY TO PROVIDE THE NEEDED SUPPORT.

PLANT MAINTENANCE

ANOTHER IMPORTANT ASPECT OF NUCLEAR POWER IS THE PHYSICAL CONDITION OF THE PLANT AND ITS HOUSEKEEPING.

NAVY EXPERIENCE OVER MANY YEARS HAS SHOWN THAT THE GENERAL CONDITION OF ANY POWER PLANT, INCLUDING EVEN SUCH APPARENTLY INCIDENTAL ITEMS AS TIDINESS OR HOUSEKEEPING, ARE IMPORTANT TO RELIABILITY AND SAFETY. THE GENERAL APPEARANCE AND CONDITION OF A PLANT IS A GOOD INDICATOR OF THE DISCIPLINE AND COMPETENCE OF THE PEOPLE WHO RUN IT. IF A HOME IS NEAT, THERE IS LESS CHANCE OF AN ACCIDENT. THE SAME CONCEPT APPLIES TO A POWER PLANT, AND THIS ATTITUDE MUST PERVADE THE ENTIRE OPERATION. PEOPLE WHO WORK IN A SLOPPY ENVIRONMENT ARE LIKELY TO ACT IN A SLOPPY MANNER.

HOUSEKEEPING IN NUCLEAR POWER PLANTS POSES A PARTICULAR PROBLEM SINCE SOME PARTS OF THE PLANT ARE INACCESSIBLE MOST OF THE TIME. EVEN DURING THE REMAINDER OF THE TIME THEY ARE DIFFICULT TO INSPECT BECAUSE OF RADIATION. NONETHELESS, THOROUGH, PERIODIC INSPECTION AND CLEANING OF THE ENTIRE PLANT AND CORRECTION OF DEFICIENCIES ARE ESSENTIAL. TO AID IN THIS, THE DISTRIBUTION OF RADIOACTIVITY IN THE PLANT MUST BE CONTROLLED. RADIOACTIVITY

THAT STAYS WITHIN THE CORE CONTRIBUTES LITTLE TO THE RADIATION RECEIVED IN WORKING AT THE PLANT. THEREFORE, THE PLANT MUST HAVE HIGH INTEGRITY FUEL ELEMENTS TO RETAIN THE RADIOACTIVE FISSION PRODUCTS.

MUCH OF THE RADIATION RECEIVED DURING PLANT MAINTENANCE COMES FROM RADIOACTIVE CORROSION PRODUCTS SUCH AS COBALT. THE AMOUNT OF THIS TYPE OF RADIOACTIVITY CAN BE MINIMIZED BY PROPER SELECTION OF MATERIALS AND CONTROL OF COOLANT CHEMISTRY. ITS LOCATION CAN BE CONTROLLED BY DETAILED DESIGN OF SYSTEMS AND COMPONENTS TO ELIMINATE LOCAL SPOTS WHERE RADIOACTIVE MATERIAL COULD ACCUMULATE. MOST IMPORTANT, AIRBORNE ACTIVITY AND RADIOACTIVE CONTAMINATION OUTSIDE THE PRIMARY COOLANT SYSTEM CAN BE MINIMIZED BY ELIMINATING ROUTINE LEAKAGE OF PRIMARY COOLANT AND BY LOCAL CONTAINMENT OF ANY TEMPORARY LEAKAGE WHICH DOES OCCUR.

IN DISCUSSING INSPECTION OF THE PLANT, I REFER PRINCIPALLY TO FINDING AND REPAIRING THE LITTLE THINGS - STEAM LEAKS, VALVE PACKING LEAKS, WETTED INSULATION, RUSTING VENTS, INOPERATIVE OR OUT OF CALIBRATION INSTRUMENTS OR COMPONENTS, ETC. ONCE A POWER PLANT IS CONSTRUCTED, IT MUST NOT JUST BE LEFT ALONE. IT REQUIRES CONTINUOUS, DETAILED ATTENTION. IT ALSO REQUIRES THAT COMPLETE RECORDS BE MAINTAINED OF THE DEFICIENCIES WHICH DO OCCUR AND HOW THEY ARE CORRECTED.

TO ENSURE THAT PLANTS ARE BEING KEPT IN GOOD CONDITION, I REQUIRE THOROUGH, PERIODIC INSPECTION - INCLUDING THE REACTOR COMPARTMENT - BY THE SENIOR OFFICERS. I ALSO HAVE SUCH INSPECTIONS MADE BY PEOPLE FROM HEADQUARTERS.

FACE FACTS

ANOTHER PRINCIPLE FOR SUCCESSFUL APPLICATION OF A SOPHISTICATED TECHNOLOGY IS TO FACE FACTS. ONE MUST BE CONSCIOUS OF AND ACTIVELY GUARD AGAINST THE HUMAN INCLINATION TO HOPE THAT THINGS WILL WORK OUT DESPITE EVIDENCE OR SUSPICIONS TO THE CONTRARY. ONE IMPORTANT WAY TO DO THIS IS TO HOLD PEOPLE ACCOUNTABLE FOR LONG-TERM PERFORMANCE. ONE WHO KNOWS HE WILL BE HELD ACCOUNTABLE IF THINGS DO NOT WORK RELIABLY IS MORE LIKELY TO RESIST SHORT-TERM OPTIMISM THAN ONE WHO KNOWS HE WILL NOT. A MANAGER WHO IS EVALUATED ON SHORT-TERM RESULTS ALONE IS LESS LIKELY TO FACE THE FACTS AND ACT WHEN THE CORRECTIVE ACTION IS UNPALATABLE AND COSTLY. I HAVE ALWAYS ACTED IN EACH JOB I HAVE HAD AS IF I WOULD HOLD IT AND BE HELD RESPONSIBLE FOREVER - EVEN ON JUDGEMENT DAY - AND PERHAPS BEYOND.

IF THINGS DO NOT APPEAR TO BE QUITE RIGHT, YOU MUST DIG OUT THE FACTS AND MAKE NEEDED CHANGES DESPITE SIGNIFICANT COSTS AND SCHEDULE DELAYS. A NUMBER OF TIMES DURING THE COURSE OF MY WORK I HAVE MADE DECISIONS TO STOP WORK AND REDESIGN OR REBUILD EQUIPMENT - NO MATTER WHAT THE DELAY OR COST - TO PROVIDE THE

REQUISITE ASSURANCE OF SATISFACTORY PERFORMANCE. ON SOME OCCASIONS, I HAVE FOUND IT NECESSARY TO REPLACE PERSONNEL.

THE MAN IN CHARGE MUST PERSONALLY SET THE EXAMPLE IN THIS AREA AND REQUIRE HIS SUBORDINATES TO DO LIKEWISE. THOSE WHO WILL NOT OR CAN NOT DO THIS MUST BE REPLACED.

POSSIBILITY OF MISTAKES MUST BE TAKEN INTO ACCOUNT

WHAT I HAVE PRESENTED UP TO THIS POINT AND THE INFORMATION I FURNISHED TO YOU IN MY MAY 24TH STATEMENT INDICATE SOME OF WHAT I DO IN RUNNING THE NAVAL REACTORS PROGRAM. EVEN WHEN THESE MEASURES ARE CARRIED OUT, MISTAKES WILL BE MADE AND EQUIPMENT WILL FAIL, BECAUSE WE ARE DEALING WITH MACHINES AND THEY CANNOT BE MADE PERFECT. THE HUMAN BODY IS GOD'S FINEST CREATION WE KNOW OF AND YET IT IS NOT PERFECT - WE GET SICK. WE CANNOT EXPECT, PHILOSOPHICALLY, THAT MACHINES WILL BE MORE NEARLY PERFECT THAN THE HUMAN BEINGS WHO CREATE THEM.

NUCLEAR POWER CAN BE SAFELY USED

IF THE PRINCIPLES I HAVE OUTLINED ARE CARRIED OUT WITH STEADFAST COMMITMENT, I BELIEVE NUCLEAR POWER CAN BE SAFELY USED, EVEN TAKING INTO ACCOUNT MISTAKES THAT WILL INEVITABLY OCCUR. THAT IS THE BASIS ON WHICH I HAVE CONDUCTED ALL MY WORK AND I BELIEVE IT JUST AS STRONGLY TODAY AS I EVER HAVE.

SOME SUGGESTED ACTIONS

LET ME NOW SUMMARIZE SOME SPECIFIC ACTIONS I SUGGEST BE CONSIDERED, AND COMMENT ON SOME OTHERS WHICH I UNDERSTAND HAVE BEEN SUGGESTED:

1. UTILITY MANAGEMENT AS THE OWNERS AND OPERATORS OF THE PLANTS HAVE PRIME RESPONSIBILITY FOR THEIR SAFETY. THEY MUST ACCEPT THEIR RESPONSIBILITY AND BECOME KNOWLEDGEABLE IN THE TECHNICAL FACETS OF NUCLEAR POWER. THE UTILITIES SHOULD UPGRADE THEIR TECHNICAL STAFF AND GIVE THEM DIRECT AND FREQUENT ACCESS TO TOP MANAGEMENT. THE STAFF SHOULD HAVE FULL RESPONSIBILITY FOR SAFETY INCLUDING DESIGN AND TRAINING AS WELL AS OPERATIONAL MATTERS, AND SHOULD HAVE THE AUTHORITY TO TAKE THE NECESSARY ACTIONS. TECHNICAL DECISIONS MUST BE MADE ON A TECHNICAL BASIS. THEY CANNOT BE MADE BY PURCHASING AGENTS, COMPTROLLERS OR LAWYERS. I HAVE CONTRACT AND BUDGET PEOPLE. BUT THESE PEOPLE SERVE THE TECHNICAL GROUPS - THEY DO NOT RUN THE PROGRAM OR OVERRIDE TECHNICAL CONSIDERATIONS.

FOR MANY YEARS I HAVE RECOMMENDED THAT THE UTILITIES UNITE TO ESTABLISH A SEPARATE TECHNICAL ORGANIZATION WHICH COULD PROVIDE A MORE COORDINATED AND EXPERT TECHNICAL INPUT AND CONTROL FOR THE COMMERCIAL NUCLEAR POWER PROGRAM THAN IS PRESENTLY POSSIBLE FOR EACH UTILITY WITH ITS LIMITED STAFF. THE ELECTRIC POWER RESEARCH INSTITUTE, EPRI, IS AN EXAMPLE OF THIS. IT

PERFORMS RESEARCH AND DEVELOPMENT IN TECHNOLOGY ASSOCIATED WITH NUCLEAR POWER AND OTHER FORMS OF POWER GENERATION. I UNDERSTAND THAT A SIMILAR ARRANGEMENT IS BEING MADE IN THE AREA OF OPERATOR TRAINING. THESE ARE GOOD STEPS - BUT NOT ENOUGH. THE CENTRAL TECHNICAL ORGANIZATION I RECOMMEND SHOULD HAVE A CLEAR MANDATE FOR SAFETY ASPECTS AS A PART OF ITS FUNCTION. AMONG THE THINGS SUCH AN ORGANIZATION COULD DO ARE:

A. DEVELOP THE STANDARDS AND SPECIFICATIONS UTILITIES SHOULD REQUIRE FOR DESIGN AND CONSTRUCTION OF THEIR PLANTS.

B. PROVIDE DIRECT, IN-DEPTH TECHNICAL ASSISTANCE TO UTILITIES IN DESIGN, CONSTRUCTION AND OPERATIONAL QUESTIONS.

C. ESTABLISH RECOMMENDED STAFFING REQUIREMENTS FOR OPERATION OF NUCLEAR PLANTS. FOR EXAMPLE, I UNDERSTAND THAT AT TIMES THERE MAY BE ONLY A SINGLE OPERATOR WITH NO SUPERVISION PRESENT IN THE CONTROL ROOM OF AN OPERATING PLANT. ALSO, THAT OPERATORS MAY BE ASSIGNED AND ACTUALLY CARRY OUT UNRELATED DUTIES WHILE ON WATCH. THESE ARE CONTRARY TO NAVY PRACTICE.

D. DEVELOP A COMPREHENSIVE TRAINING AND RETRAINING PROGRAM, INCLUDING LESSON PLANS, QUALIFICATION REQUIREMENTS, ETC. FOR UTILITIES TO USE IN TRAINING THEIR PEOPLE. THIS MUST BE BASED ON WHAT IS NEEDED AND NOT GEARED SOLELY TO PASSING LICENSING EXAMINATIONS. IT SHOULD COVER ALL TYPES OF PERSONNEL, NOT JUST OPERATORS.

E. PROVIDE TRAINED TECHNICAL TEAMS TO PERFORM PERIODIC AUDITS OF NUCLEAR STATIONS AND CRITICALLY EVALUATE THE PLANTS AND QUALIFICATION AND PERFORMANCE OF PERSONNEL.

F. ADVISE UTILITIES ON TECHNICAL SAFETY QUESTIONS.

OTHER FUNCTIONS PROBABLY WOULD BECOME APPARENT IN TIME.

THE CONTRIBUTION SUCH AN ORGANIZATION COULD MAKE WOULD BE CONSIDERABLE IF GIVEN THE PERSONNEL AND AUTHORITY TO CONCENTRATE ON THE TECHNICAL ASPECTS, WITHOUT UNDUE CONCERN FOR ISSUES SUCH AS SCHEDULES, ECONOMICS AND THE LIKE. IF THEY ARE SET UP TO BE JUST A MOUTHPIECE FOR JUSTIFYING WHATEVER THE UTILITIES WANT TO DO BASED ON PROFIT AND LOSS, AS IS THE CASE WITH MANY INDUSTRY ORGANIZATIONS, IT WILL BE A WASTED EFFORT. ALSO, IF UTILITIES MANAGEMENT SIMPLY TURN OVER ALL TECHNICAL MATTERS TO THIS ORGANIZATION, IT WILL NOT WORK. UTILITIES ALSO NEED THEIR OWN IN-HOUSE TECHNICAL COMPETENCE.

IN SETTING UP SUCH AN ORGANIZATION, CARE MUST BE TAKEN TO GET THE PROPER PEOPLE. IT IS MORE IMPORTANT THAT THEY HAVE A PROVEN RECORD OF <u>ACTUAL</u> ACCOMPLISHMENT IN A PRACTICAL, SUCCESSFUL APPLICATION OF TECHNOLOGY THAN THAT THEY BE "EXPERTS" OR "SENIOR STATESMEN" WHO HAVE BECOME WELL KNOWN BECAUSE THEY HAVE DONE A LOT OF TALKING FOR MANY YEARS ABOUT THE NUCLEAR POWER FIELD. MANY "EXPERTS" HAVE A FAR BETTER REPUTATION THAN THEIR ACTUAL ACCOMPLISHMENTS WARRANT. CONSIDERATION SHOULD BE GIVEN TO

WHETHER TOP PEOPLE TO BE SELECTED FOR SUCH ORGANIZATIONS FORESAW THE PRESENT PROBLEMS AND TOOK STEPS TO HANDLE THEM IN PROGRAMS FOR WHICH THEY WERE RESPONSIBLE BEFORE THEY ACHIEVED THE REPUTATION OF "EXPERTS". IN OTHER WORDS, THEY SHOULD BE JUDGED ON ACTIONS AND RESULTS, NOT ON VERBAL ABILITY. THE BIBLE SAYS IN PROVERBS "EVEN A CHILD IS KNOWN BY HIS DOINGS.... AND WHETHER IT BE RIGHT".

2. THE CONCEPT OF PERSONAL RESPONSIBILITY MUST BE APPLIED. FUNDAMENTAL TO THIS CONCEPT OF PERSONAL RESPONSIBILITY IN NUCLEAR POWER OR ANY ENGINEERING ENDEAVOR IS UNDERSTANDING AND PROPERLY INTERPRETING TECHNICAL FACTS IN MAKING DECISIONS. RELIANCE ON "MANAGEMENT TECHNIQUES" HAS BECOME RAMPANT THROUGHOUT GOVERNMENT AND INDUSTRY. SO LONG AS THE PEOPLE IN CHARGE MAKE DECISIONS WITHOUT UNDERSTANDING THE TECHNICAL ISSUES, A LACK OF PERSONAL RESPONSIBILITY WILL OBTAIN. HOW CAN ANYONE WHO DOES NOT UNDERSTAND THE TECHNICAL ASPECTS OF WHAT HE IS DOING REALLY BE RESPONSIBLE OR FEEL PERSONALLY RESPONSIBLE? IF YOU KNOW AN AUTO MECHANIC WHO TAKES PERSONAL RESPONSIBILITY FOR HIS WORK, ISN'T IT BECAUSE HE KNOWS EVERY FACET OF ENGINES AND HOW TO MAKE THEM WORK? UNTIL THIS BASIC FACT IS RECOGNIZED AND ACCEPTED, WE CANNOT REALLY GET PERSONAL RESPONSIBILITY IN ANY TECHNICAL AREA. WHILE I AM NOT PERSONALLY FAMILIAR WITH THE SPECIFICS, NEWSPAPER ARTICLES SUGGEST THAT CURRENT PROBLEMS WITH THE NEW YORK SUBWAYS CAME ABOUT BECAUSE NON-TECHNICAL MANAGEMENT OVERRULED THE ENGINEERS' TECHNICAL OBJECTIONS IN FAVOR OF SUPPOSED

COST SAVINGS. THE COST OF REPAIRS IS REPORTED TO HAVE EXCEEDED THE ESTIMATED SAVINGS ALREADY. WHEN THEY ARE SUBORDINATED IN TECHNICAL MATTERS TO ACCOUNTANTS, BUSINESS MANAGERS, LAWYERS AND BANKERS, TECHNICAL PEOPLE CANNOT BE EXPECTED TO EXERCISE PERSONAL RESPONSIBILITY.

3. THERE SHOULD BE A GOVERNMENT REPRESENTATIVE IN THE CONTROL ROOM AT ALL TIMES WITH THE AUTHORITY TO SHUT THE PLANT DOWN IF HE BELIEVES THIS TO BE NECESSARY FOR SAFETY. I HAVE ADVOCATED THIS FOR YEARS. IT PROVIDES AN INDEPENDENT MONITOR WHOSE SOLE CONCERN IS SAFETY.

4. ALL ACTIVITIES INVOLVED IN NUCLEAR POWER - UTILITIES, REACTOR VENDORS, MANUFACTURERS, AND REGULATORY AGENCIES MUST ESTABLISH AND RETAIN AS PERMANENT A STAFF AS POSSIBLE, SO LONG AS THEY PERFORM WELL. THIS IS ESSENTIAL IN THE NUCLEAR BUSINESS WHERE IT TAKES OVER TEN YEARS FROM THE TIME A PLANT IS ORDERED UNTIL IT STARTS OPERATING - AND WHERE THE PLANT IS THEN EXPECTED TO OPERATE SAFELY FOR ITS LIFE OF 30 TO 40 YEARS. WITH PERMANENCE YOU GAIN EXPERIENCE, JUDGEMENT, AND A "CORPORATE MEMORY" WHICH ARE HARD TO REPLACE.

HOWEVER, YOU CANNOT PREDICATE YOUR PROGRAM ON THE BASIS THAT PEOPLE WILL NEVER LEAVE, BECAUSE THEY DO. NO ONE IS INDISPENSABLE NOR SHOULD ANY TECHNICAL EFFORT BE PREDICATED ON ANY INDIVIDUAL BEING INDISPENSABLE. THAT IS WHY THERE MUST BE FORMAL DOCUMENTA-

TION AND WHY THOROUGH TRAINING AND AUDITING PROGRAMS ARE NECESSARY - SO THAT NEW PEOPLE CAN BE BROUGHT IN WITHOUT COMPROMISING SAFETY. TO RETAIN PEOPLE, THEY MUST BE PAID ADEQUATELY. MORE IMPORTANT, TO ATTRACT AND RETAIN GOOD TECHNICAL PEOPLE, THEY MUST BE TRAINED AND GIVEN AUTHORITY AND RESPONSIBILITY. NOTHING CAUSES TECHNICAL PEOPLE TO LEAVE MORE QUICKLY THAN NOT BEING ABLE TO DO THEIR TECHNICAL JOBS PROPERLY. UNTIL ADEQUATE RECOGNITION IS GIVEN TO TECHNICAL COMPETENCE, THE TURNOVER OF PEOPLE NEEDED FOR NUCLEAR POWER WILL BE GREATER THAN WARRANTED.

5. PLANT DESIGNS, EQUIPMENT, CONTROL ROOMS, TRAINING, ETC. SHOULD BE STANDARDIZED INSOFAR AS PRACTICABLE. I DO NOT KNOW HOW FAR IT IS POSSIBLE TO STANDARDIZE CONTROL ROOMS, INSTRUMENTATION AND OTHER FEATURES OF EXISTING PLANT DESIGNS SINCE THE PLANTS THEMSELVES ARE NOT STANDARD. CERTAINLY IT SHOULD BE POSSIBLE TO STANDARDIZE TYPES, COLORS AND SIGNIFICANCE OF ALARMS, SWITCHES, ETC. ON NEW PLANTS, MUCH MORE STANDARDIZATION IN ALL ASPECTS INCLUDING REACTOR RATING SEEM PRACTICABLE.

TO THE EXTENT IT IS PRACTICABLE TO STANDARDIZE, TWO DISTINCT BENEFITS WOULD RESULT. THE FIRST IS THAT A LARGER NUMBER OF ENGINEERING MAN HOURS COULD BE APPLIED TO THE STANDARD DESIGNS THAN TO EACH OF MANY DIFFERENT DESIGNS. THIS SHOULD RESULT IN BETTER DESIGNS. THE QUALIFICATION, TEST PROGRAM, DEVELOPMENT OF OPERATING PROCEDURES, OPERATIONAL MANUALS, TEST

PROCEDURES, AND CALIBRATION PROCEDURES SHOULD ALSO BENEFIT FROM THE INCREASED ATTENTION. FURTHER, WITH A LARGER NUMBER OF IDENTICAL OPERATING SYSTEMS, OPERATIONAL EXPERIENCE WILL PROVIDE A VALUABLE SOURCE OF INFORMATION THAT CAN BE USED TO IMPROVE THE DESIGN AND PROCEDURES AND ESTABLISH A MORE EFFECTIVE PREVENTIVE MAINTENANCE PROGRAM FOR ALL PLANTS.

THE SECOND BENEFIT OF STANDARDIZATION RELATES TO THE TRAINING OF OPERATING AND INSPECTION PERSONNEL. THE USE OF STANDARD DESIGNS WOULD MAKE IT POSSIBLE TO TRAIN OPERATING PERSONNEL MORE EFFECTIVELY AND TO CONDUCT MORE EFFECTIVE AUDITS.

IN ADVOCATING MORE STANDARDIZATION I AM NOT SAYING THAT THERE SHOULD BE ONE SINGLE DESIGN. I HAVE STANDARDIZED IN MY PROGRAM AS FAR AS PRACTICABLE. EVEN THEN WE HAVE A NUMBER OF DESIGNS TO SUIT THE DIFFERENT POWER RATINGS AND SHIP TYPES AND TO TAKE ADVANTAGE OF NEW DEVELOPMENTS AND TECHNOLOGY WHICH HAVE BECOME AVAILABLE.

6. MINIMIZE RELIANCE ON AUTOMATION AND COMPUTER CONTROL. I RECOGNIZE THAT THIS RUNS COUNTER TO THE BELIEF OF SOME, BUT MY EXPERIENCE IS THAT PRIMARY RELIANCE FOR SAFELY OPERATING A NUCLEAR POWER PLANT MUST BE PLACED ON THE OPERATOR. I AM NOT AGAINST COMPUTERS; THEY ARE IMPORTANT. FROM THE EARLIEST DAYS OF THE NAVAL REACTORS PROGRAM, THE MOST ADVNACED COMPUTERS HAVE BEEN USED IN THE DESIGN AND ANALYSIS OF OUR PLANTS. BUT IN MY

CONSIDERED OPINION, UNDUE RELIANCE ON AUTOMATION AND COMPUTERS FOR CONTROL CAN IMPAIR SAFETY.

THERE ARE SEVERAL REASONS FOR THIS: FIRST, FOR A COMPUTER TO OPERATE PROPERLY IT MUST BE PROGRAMMED PROPERLY. PROGRAMMING IS A PRE-ESTABLISHED SET OF INSTRUCTIONS. FOR A COMPUTER TO BE EFFECTIVE UNDER EMERGENCY CONDITIONS REQUIRES THAT THE CASUALTY AND THE SEQUENCE OF INFORMATION EXPECTED FROM THE COMPUTER HAVE BEEN DEFINED IN ADVANCE. MOST MAJOR PROBLEMS RESULT FROM UNEXPECTED EVENTS WHICH CHANGED A PREDICTED EVENT INTO AN EVENT OR SEQUENCE OF EVENTS NOT COVERED BY PREVIOUS EXPERIENCE.

IF IT IS POSSIBLE TO PREDICT COMPLICATED CASUALTIES IN ADVANCE, IT IS BETTER TO TAKE ACTION TO CORRECT THE DESIGN TO PREVENT OR MODERATE THE CASUALTIES THAN TO ADD ADDITIONAL EQUIPMENT SUCH AS COMPUTERS TO TRY TO CONTROL THEM.

THE EMPHASIS SHOULD BE NOT ON MORE COMPLICATED AND SOPHISTICATED CONTROL BUT ON DESIGNING AND BUILDING A SIMPLE, STABLE PLANT. AN INHERENTLY STABLE REACTOR MAKES FEWER DEMANDS ON THE CONTROL SYSTEM AND THE OPERATORS. THEREFORE, IT RESULTS IN A SIMPLER MORE RELIABLE PLANT - ONE WITH A LARGE DEGREE OF "FORGIVENESS" BUILT INTO IT. WITH SUCH A REACTOR, IT IS POSSIBLE FOR AN OPERATOR TO DEVELOP A FEELING FOR PLANT PERFORMANCE AND BEHAVIOR. HE CAN THEN RECOGNIZE ABNORMAL BEHAVIOR AND HAVE TIME TO INITIATE CORRECTIVE ACTION.

SECOND, FOR CASUALTIES WHICH DO OCCUR, THE OPERATOR MUST HAVE AVAILABLE, IN A MANNER HE CAN UNDERSTAND, INFORMATION RELATING TO THE ESSENTIAL PLANT PARAMETERS. PLACING A COMPUTER BETWEEN THE OPERATOR AND THE REACTOR PLANT IS EQUIVALENT TO PLACING A FILTER BETWEEN THE OPERATOR AND THE CASUALTY. THIS FILTER CAN PREVENT THE OPERATOR FROM HAVING ESSENTIAL INFORMATION AVAILABLE.

THIRD, ANY COMPUTERS USED CONSTITUTE ADDITIONAL SOURCES OF ERROR OR MALFUNCTIONS WHICH CAN MISLEAD THE OPERATOR RELYING ON THEM. THIS IS PARTICULARLY TRUE IN AN EMERGENCY WHEN THE TIME TO TAKE CORRECTIVE MEASURES IS AT A MINIMUM.

FINALLY, THE VERY EXISTENCE OF THE COMPUTER OR AUTOMATIC CONTROL LEADS THE OPERATOR AND OTHERS INVOLVED IN OPERATION, DESIGN, AND TRAINING TO RELY ON THE "MAGIC" IT PROVIDES. THIS DIVERTS NEEDED ATTENTION FROM OTHER AREAS.

IN THE FINAL ANALYSIS, WE MUST DEPEND ON HUMAN BEINGS. NO MACHINE, INCLUDING A COMPUTER, CAN BE MORE PERFECT THAN THE HUMAN BEINGS WHO DESIGNED IT, USE IT, OR RELY ON IT.

7. SIMPLIFY AND REDUCE THE SIZE OF CONTROL ROOMS. EVEN RECOGNIZING THE DIFFERING REQUIREMENTS FOR NAVAL AND CIVILIAN NUCLEAR POWER PLANTS THERE ARE SEVERAL THINGS I HAVE READ ABOUT THE CONTROL ROOM AT THREE MILE ISLAND WHICH WERE A SURPRISE TO ME. I UNDERSTAND THAT MOST IF NOT ALL OF THEM WERE IDENTIFIED IN AN ELECTRIC POWER RESEARCH INSTITUTE REPORT OF NOVEMBER 1976

TITLED "HUMAN FACTORS REVIEW OF NUCLEAR POWER PLANT CONTROL ROOM DESIGN". THE REPORT IDENTIFIED SUCH PROBLEMS AS PHYSICAL SIZE OF THE CONTROL PANELS, NUMBER OF GAUGES AND ALARMS, ARRANGEMENT AND MARKING OF ALARMS, GAUGES AND CONTROLS. IT WOULD BE WORTHWHILE TO LEARN WHAT ACTION WAS TAKEN AS A RESULT OF THAT REPORT. IN THE NAVAL REACTORS PROGRAM, WE MINIMIZE THE NUMBER AND TYPES OF INSTRUMENTS AND ALARMS NEEDED. THIS RESULTS IN MUCH SMALLER CONTROL ROOMS.

8. DO NOT DIVIDE RESPONSIBILITY. FOR EXAMPLE, IT HAS BEEN SUGGESTED THAT AN AGENCY OTHER THAN THE PLANT OWNER EMPLOY THE OPERATORS OR THAT AN AGENCY OTHER THAN THE NUCLEAR REGULATORY COMMISSION (NRC) BE RESPONSIBLE FOR REGULATING OPERATOR TRAINING. I DO NOT SUPPORT EITHER OF THESE PROPOSALS. CONTROL ROOM OPERATORS SHOULD BE EMPLOYED BY THOSE WHO OWN AND OPERATE THE PLANTS. RESPONSIBILITY FOR SELECTING AND TRAINING OPERATORS SHOULD NOT BE SEPARATED FROM RESPONSIBILITY FOR DESIGN, MAINTENANCE, AND OPERATION OF THE PLANT. WITHIN THE EXISTING FRAMEWORK IT SEEMS APPROPRIATE TO ME THAT THE NUCLEAR REGULATORY COMMISSION ESTABLISH THE NECESSARY REQUIREMENTS FOR PERSONNEL QUALIFICATION AND TRAINING. IT IS THEN UP TO THE UTILITIES TO PROVIDE ADEQUATE TRAINING - SUBJECT TO NRC OVERSIGHT.

9. IT HAS BEEN SUGGESTED THAT ALL INSTRUMENTATION FOR NUCLEAR POWER PLANTS BE REQUIRED TO BE "DIRECT READING" AND

THAT ALL MONITORING SYSTEMS INDICATE WHETHER A CONTROL FUNCTION ACTUALLY HAS BEEN PERFORMED - RATHER THAN WHETHER THE CONTROL SIGNAL HAS BEEN GIVEN. I DO NOT AGREE WITH SUCH GENERALIZED REQUIREMENTS ON SPECIFIC DESIGN FEATURES.

INSTRUMENTATION USED FOR REACTOR PLANTS MUST BE RELIABLE AND READILY MAINTAINED AND CALIBRATED. SOMETIMES, SO-CALLED "DIRECT READING" INSTRUMENTATION CANNOT PROVIDE THE ABOVE FEATURES. ALSO, SO-CALLED "DIRECT READING" INSTRUMENTATION CAN BE AS SUBJECT TO MISUNDERSTANDING OR FAILURE AS CAN ANY OTHER INSTRUMENTATION. FOR EXAMPLE, REACTOR FLOW CAN BE MEASURED "DIRECTLY" BY A FLOW METER - A METER WHICH, IN ACTUALITY, MEASURES NOT FLOW BUT PRESSURE DROP ACROSS A SECTION OF PIPE - OR IT CAN BE INFERRED BY MEASUREMENTS OF TEMPERATURE, PUMPING POWER, OR PUMP SPEED. MEASURING THE FLOW DIRECTLY IS NOT NECESSARY TO ASSURE SAFE OPERATION OF THE REACTOR AND REQUIRES ADDITIONAL COMPLICATING EQUIPMENT AND INSTRUMENTS.

SIMILARLY, IT IS DESIRABLE IN MANY CASES THAT MONITORING SYSTEMS INDICATE THAT A CONTROL FUNCTION HAS BEEN PERFORMED RATHER THAN THAT THE COMMAND SIGNAL HAS BEEN SENT TO THE DEVICE IN QUESTION. HOWEVER, IN SOME CASES, IT IS IMPRACTICABLE TO PROVIDE THIS INDICATION. FOR THOSE CASES, OPERATING PERSONNEL SHOULD BE TRAINED TO LOOK FOR OTHER INDICATIONS WHICH SHOW WHETHER THE CONTROL FUNCTION HAS OCCURRED.

AGAIN, IT IS POSSIBLE TO PROVIDE TOO MUCH INSTRUMENTATION; THIS WILL CONFUSE THE OPERATORS OR, IF THE INSTRUMENTATION IS NOT RELIABLE, OPERATING PERSONNEL WILL DISTRUST IT AND NOT BELIEVE ITS INDICATIONS WHEN THEY SHOULD.

WHAT INSTRUMENTS ARE REQUIRED TO ASSURE SAFE OPERATION OF THE REACTOR MUST BE DETERMINED FOR EACH SPECIFIC REACTOR AND PLANT DESIGN.

10. THE UTILITIES MUST PLAY THE MAJOR ROLE IN ACHIEVING EFFECTIVE USE OF IMPROVED SPECIFICATION CODES AND STANDARDS. I KNOW THERE ARE SPECIFICATION AND STANDARDS PROGRAMS UNDERWAY FOR COMMERCIAL NUCLEAR POWER. THERE ARE THREE THOUGHTS I WOULD LIKE TO GIVE YOU RELATIVE TO SUCH PROGRAMS:

<u>FIRST</u>, THERE IS NO USE HAVING SPECIFICATIONS, CODES OR STANDARDS IF THEY ARE NOT INVOKED AND ENFORCED. IN FACT, IF THEY ARE NOT ENFORCED, THEY ARE HARMFUL BECAUSE THEIR EXISTENCE IS CONSOLING TO THOSE IN AUTHORITY AND GIVES THEM UNWARRANTED ASSURANCE. THERE MUST BE AN EFFECTIVE WAY TO SEE THAT THE PROPER REQUIREMENTS ARE IN FACT INVOKED AND ENFORCED, AND THAT THERE IS PROPER TECHNICAL CONTROL OVER ANY WAIVER. IN THIS REGARD, THE CUSTOMER - THE UTILITY - MUST TAKE THE LEAD.

<u>SECOND</u>, SPECIFICATIONS MUST BE KEPT UP-TO-DATE. KNOWLEDGE AND TECHNOLOGY ARE INCREASING RAPIDLY. WE REVISE OUR SPECIFICATION CODES AND STANDARDS PROMPTLY IN RESPONSE TO SPECIFIC PROBLEMS OR NEW INFORMATION. WE ALSO REVIEW EVERY SPECIFICATION EVERY YEAR AND WE FIND IT NECESSARY TO CHANGE ABOUT ONE THIRD OF THEM EACH YEAR.

Third, most if not all industry codes and standards represent a "consensus". In practice, the suppliers, not the customers, dominate development of these standards. That may be proper for clothes pins and light bulbs but not for nuclear power plants. As the person responsible for Navy plants, I have had to establish requirements on material and equipment which our suppliers would not agree to meet. Initially, I had to take the risk of paying for an item and then not using it because it did not meet what was required. Later, when the suppliers had seen that the requirements could be met, they would accept them. However, if I had waited for "consensus" on the requirements or relied on existing or proposed industry standards to assure adequacy, I would never have obtained the needed improvements.

Navy specifications and manuals are not directly applicable to commercial nuclear power because of special military requirements. However, the principle that the customer must be technically knowledgeable and base his specifications on what is needed does apply.

11. Do not succumb to calls for more research and development as a response to the Three Mile Island incident. There are always contractors seeking large sums of federal money to spend on interesting research. By supporting that idea we can give lip service to the problem and promise that by offering up money today,

A SOLUTION WILL BE FOUND BY SOME R&D ORGANIZATION IN THE FUTURE. BUT IN MY OPINION, SUCH ACTION WILL ONLY OBSCURE THE REAL PROBLEMS AND DELAY THEIR SOLUTION.

SOME SPECIFIC AREAS MAY WARRANT RESEARCH AND DEVELOPMENT BUT THAT IS A MINOR PART OF WHAT IS NEEDED. IF ANYTHING, THERE HAS BEEN TOO MUCH EMPHASIS ON RESEARCH AND DEVELOPMENT IN NUCLEAR POWER AND NOT ENOUGH ON THE DAILY DRUDGERY OF SEEING THAT EVERY ASPECT OF NUCLEAR POWER IS IN FACT BEING PROPERLY HANDLED EVERY DAY BY EACH OF THE ORGANIZATIONS INVOLVED. THAT IS WHERE THE EMPHASIS IS NEEDED.

ALL HUMAN ACTS INVOLVE RISKS

I WOULD LIKE TO MAKE A PHILOSOPHIC POINT WHICH SHOULD BE UNDERSTOOD.

NOTHING THAT WE DO IS WITHOUT RISK. FOR EXAMPLE, WE ACCEPT THE INEVITABILITY OF AUTOMOBILE ACCIDENTS. SINCE THE THREE MILE ISLAND ACCIDENT, WE HAVE SEEN THE CRASH OF A DC-10, FAILURES IN NEW YORK SUBWAYS, RELEASE OF TOXIC MATERIAL FROM TRAIN ACCIDENTS, AND MANY OTHER RESULTS OF MAN'S ACTIONS. SEVERAL OF THESE INCIDENTS RESULTED IN LOSS OF HUMAN LIFE. SOME HAVE INVOLVED EVACUATION OF ADJACENT AREAS.

EVEN SUCH WIDELY HERALDED CONSIDERATIONS AS THE LONG LIFE OF NUCLEAR WASTES AND THE POSSIBILITY OF GENETIC EFFECTS IN FUTURE GENERATIONS ARE NOT UNIQUE TO NUCLEAR POWER. THERE IS INCREASING RECOGNITION THAT FOSSIL FUELS MAY CAUSE A PERMANENT ADVERSE CHANGE IN OUR CLIMATE DUE TO THE PRODUCTION OF CARBON DIOXIDE - THE "GREENHOUSE" EFFECT. THE APPARENT "LIFETIME" OF CARBON DIOXIDE IS LONG IN TERMS OF OUR OWN LIFE SPAN AND THE QUANTITIES INVOLVED ARE FAR GREATER THAN THE QUANTITY OF RADIOACTIVE WASTE. TO MY KNOWLEDGE, THERE IS NO EFFORT UNDERWAY EVEN TO ATTEMPT TO ISOLATE SUCH WASTES FROM THE ENVIRONMENT.

ALSO, I UNDERSTAND, MANY OF THE CHEMICAL SUBSTANCES WIDELY USED TODAY HAVE POTENTIAL GENETIC EFFECTS WITH IMPLICATIONS FOR FUTURE GENERATIONS.

NUCLEAR POWER INVOLVES POTENTIAL RISKS TO LARGE NUMBERS OF PEOPLE. IT WOULD BE WRONG TO IGNORE THOSE RISKS OR TO IMPLY THAT THEY CAN BE REDUCED TO ZERO. YOU CANNOT MORALIZE TECHNOLOGY. YOU CAN ALWAYS FIND WHERE HUMAN BEINGS HAVE ERRED. HOWEVER, THE CARE AND ATTENTION WHICH HAVE BEEN DEVOTED TO MINIMIZING THE RISKS OF NUCLEAR POWER HAVE BEEN GREAT. THE REAL QUESTIONS ARE -

WHAT MORE CAN AND SHOULD BE DONE TO REDUCE THE RISKS?
HOW CAN WE ASSURE THE NEEDED ACTIONS ARE IN FACT CARRIED OUT?
ARE THE REMAINING RISKS WORTH THE BENEFITS?

DECISION ON NUCLEAR POWER

NUCLEAR POWER IS DIFFICULT TO DEAL WITH. IT INVOLVES ENERGY - A VITAL ELEMENT IN OUR LIFE TODAY. IT INVOLVES INDIVIDUALS' CONCERNS FOR THEMSELVES AND THEIR FAMILIES, AND IT IS A HIGHLY TECHNICAL, SOPHISTICATED TECHNOLOGY. ULTIMATELY, THE DECISION AS TO WHETHER WE WILL HAVE NUCLEAR POWER IS A POLITICAL ONE - IN THE TRUE SENSE OF THE WORD - THAT IS, ONE MADE BY THE PEOPLE THROUGH THEIR ELECTED REPRESENTATIVES. IT IS ESSENTIAL THAT THE DECISION BE MADE ON THE BASIS OF FACT, NOT RHETORIC, NOR CONJECTURE OR HOPE, OR AS A RESULT OF THE WIDE-SPREAD TENDENCY TO SENSATIONALIZE THE CURRENT TOPIC AND IGNORE THE TRUE LIMITS OR RISKS OF THE ALTERNATIVES.

I AM NOT AN EXPERT OR SPECIFICALLY KNOWLEDGEABLE ABOUT ENVIRONMENTAL EFFECTS OF OTHER FORMS OF POWER GENERATION. HOWEVER, I AM AWARE THAT KNOWLEDGEABLE PEOPLE HAVE CONCLUDED THAT THE TOTAL RISK INVOLVED IN THE USE OF NUCLEAR POWER IS NO GREATER THAN THAT OF ANY ALTERNATE SOURCE WHICH CAN BE TAPPED IN THE NEXT FEW DECADES.

I REMEMBER THE OPTIMISTIC PROJECTIONS MADE FOR NUCLEAR POWER WHEN IT WAS FIRST BEING DEVELOPED. THESE SPRANG FROM HOPE AND FROM IGNORANCE OF THE ENGINEERING PROBLEMS THAT WOULD BE ENCOUNTERED IN USING NUCLEAR POWER. THERE IS NO REASON TO BELIEVE THAT CURRENT OPTIMISTIC PROJECTIONS FOR ALTERNATE MEANS OF PROVIDING LARGE AMOUNTS OF POWER ARE MORE PRECISE. TODAY, MANY

ARE TALKING OF THE EXTENSIVE USE OF COAL WITHOUT ADDRESSING THE PROBLEMS OF MINING, TRANSPORTATION, AND SAFETY; THOSE WHO ENVISION SOLAR AND OTHER SO-CALLED "NATURAL" SOURCES OF ENERGY WITHOUT CONSIDERING THEIR INHERENT LIMITATIONS AND THE DEMANDS THEY MAKE ON OTHER RESOURCES; THOSE WHO ADVOCATE EXPLOITATION OF SHALE OIL DEPOSITS WITHOUT MENTIONING THE VAST AMOUNTS OF WATER REQUIRED. ANY LARGE-SCALE GENERATION OF POWER INVOLVES MAJOR ENGINEERING DIFFICULTIES AND POTENTIAL ENVIRONMENTAL IMPACTS. NUCLEAR POWER IS NOT UNIQUE IN THIS RESPECT.

YOUR JOB IS NOT EASY. I HOPE YOU WILL FIND THE WISDOM TO MAKE THE RIGHT JUDGEMENTS AND RECOMMENDATIONS. I ALSO HOPE THAT MY COMMENTS WILL CONTRIBUTE TO YOUR DELIBERATIONS.

IN CLOSING, I WANT TO POINT OUT THE DEBT I OWE TO THE MANY, MANY PEOPLE WHO HAVE SUPPORTED ME AND THE NAVAL NUCLEAR PROGRAM OVER THE YEARS. WITHOUT THE SUPPORT OF CONGRESS, PARTICULARLY THE JOINT COMMITTEE ON ATOMIC ENERGY, THERE WOULD NOT BE A NUCLEAR NAVY AS WE KNOW IT TODAY.

SIMILARLY, I HAVE BEEN GIVEN STRONG SUPPORT BY THE DEPARTMENT OF ENERGY AND ITS PREDECESSOR AGENCIES, THE ENERGY RESEARCH AND DEVELOPMENT ADMINISTRATION AND THE ATOMIC ENERGY COMMISSION. OF THOSE IN THE DEPARTMENT OF ENERGY, I SHOULD MENTION PARTICULARLY DR. SCHLESINGER, DR. DEUTCH, MR. MYERS AND MR.

FERGUSON WHOSE SUPPORT HAS BEEN AND CONTINUES TO BE INVALUABLE.

THE DIRECT ROLE OF THE DEPARTMENT OF ENERGY IN THE NAVAL REACTORS PROGRAM HAS BEEN AND WILL CONTINUE TO BE ESSENTIAL IF WE ARE TO MAINTAIN THE SAFETY AND THE ENVIRONMENTAL ACCEPTABILITY OF THE NAVAL NUCLEAR PROGRAM.