

79604353

NUCLEAR POWERPLANT SAFETY SYSTEMS

HEARINGS
BEFORE THE
SUBCOMMITTEE ON
ENERGY RESEARCH AND PRODUCTION
OF THE
COMMITTEE ON
SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
NINETY-SIXTH CONGRESS
FIRST SESSION

—
MAY 22, 23, 24, 1979
—

[No. 32]
—

Printed for the use of the
Committee on Science and Technology



5711632

U.S. GOVERNMENT PRINTING OFFICE

48-721 O

WASHINGTON : 1979

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C., 20402

COMMITTEE ON SCIENCE AND TECHNOLOGY

DON FUQUA, Florida, *Chairman*

ROBERT A. ROE, New Jersey
MIKE McCORMACK, Washington
GEORGE E. BROWN, Jr., California
JAMES H. SCHEUER, New York
RICHARD L. OTTINGER, New York
TOM HARKIN, Iowa
JIM LLOYD, California
JEROME A. AMBRO, New York
MARILYN LLOYD BOUQUARD, Tennessee
JAMES J. BLANCHARD, Michigan
DOUG WALGREN, Pennsylvania
RONNIE G. FLIPPO, Alabama
DAN GLICKMAN, Kansas
ALBERT GORE, Jr., Tennessee
WES WATKINS, Oklahoma
ROBERT A. YOUNG, Missouri
RICHARD C. WHITE, Texas
HAROLD L. VOLKMER, Missouri
DONALD J. PEASE, Ohio
HOWARD WOLPE, Michigan
NICHOLAS MAVROULES, Massachusetts
BILL NELSON, Florida
BERYL ANTHONY, Jr., Arkansas
STANLEY N. LUNDINE, New York
ALLEN E. ERTEL, Pennsylvania
KENT HANCE, Texas

JOHN W. WYDLER, New York
LARRY WINN, Jr., Kansas
BARRY M. GOLDWATER, Jr., California
HAMILTON FISH, Jr., New York
MANUEL LUJAN, Jr., New Mexico
HAROLD C. HOLLENBECK, New Jersey
ROBERT K. DORNAN, California
ROBERT S. WALKER, Pennsylvania
EDWIN B. FORSYTHE, New Jersey
KEN KRAMER, Colorado
WILLIAM CARNEY, New York
ROBERT W. DAVIS, Michigan
TOBY ROTH, Wisconsin
DONALD LAWRENCE RITTER,
Pennsylvania
BILL ROYER, California

HAROLD A. GOULD, *Executive Director*
PHILIP B. YEAGER, *General Counsel*
REGINA A. DAVIS, *Chief Clerk*
PAUL A. VANDER MYDE, *Minority Staff Director*

SUBCOMMITTEE ON ENERGY RESEARCH AND PRODUCTION

MIKE McCORMACK, Washington, *Chairman*

MARILYN LLOYD BOUQUARD, Tennessee
ROBERT A. ROE, New Jersey
STANLEY N. LUNDINE, New York
ROBERT A. YOUNG, Missouri
RICHARD C. WHITE, Texas
HOWARD WOLPE, Michigan
RNNIE G. FLIPPO, Alabama
NICHOLAS MAVROULES, Massachusetts
RICHARD L. OTTINGER, New York
BERYL ANTHONY, Jr., Arkansas

JOHN W. WYDLER, New York
EDWIN B. FORSYTHE, New Jersey
TOBY ROTH, Wisconsin
BARRY M. GOLDWATER, Jr., California
MANUEL LUJAN, Jr., New Mexico
HAROLD C. HOLLENBECK, New Jersey

CONTENTS

WITNESSES

	Page
May 22, 1979:	
Dr. Joseph Dietrich, chief scientist, Nuclear Power Systems, Combustion Engineering	6
Milton Levenson, director, Nuclear Power Division, Electric Power Research Institute	16
William Kennedy, vice president and director of engineering, Stone & Webster Engineering Corp	26
Dr. Chauncey Kepford, director, Environmental Coalition on Nuclear Power	30
Saul Levine, director, Office of Nuclear Regulatory Research, Nuclear Regulatory Commission	92
Dr. Harold W. Lewis, professor of physics, University of California	117
Appendix I:	
Questions and answers for the record	136
Appendix II:	
Additional material for the record	247
May 23, 1979:	
Glen J. Schoessow, professor of nuclear engineering, University of Florida, accompanied by Dr. John G. Stampelos and Fred Domerow	332
Hon. John W. Wydler, U.S. Representative from the State of New York ...	342
John Macmillan, vice president, Nuclear Power Generation Division, Babcock & Wilcox Co., accompanied by Donald Roy, Manager, Engineering, Nuclear Power Generation Division	343
Herman Dieckamp, president, General Public Utilities Corp	411
Hon. William W. Scranton III, lieutenant governor, Commonwealth of Pennsylvania	425
Harold Denton, director, Office of Nuclear Reactor Regulation, Nuclear Regulatory Commission, accompanied by Roger Mattson, director, Division of System Safety, Nuclear Regulatory Commission, and Frank Congel, acting branch chief, Radiological Assessment Branch, Nuclear Regulatory Commission	453
Appendix I:	
Questions and answers for the record	496
May 24, 1979:	
Dr. Lars Larsson, technical and scientific attaché, The Swedish Embassy, accompanied by Ingmar Tiren, Manager, Nuclear Safety and Licensing (ASEA-ATOM), Vasteran, Sweden	857
George M. Low, president, Rensselaer Polytechnic Institute	880
Adm. H. G. Rickover, USN, director, Naval Nuclear Propulsion Program..	917
Appendix I:	
Additional material for the record	1178

NUCLEAR POWERPLANT SAFETY SYSTEMS

TUESDAY, MAY 22, 1979

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ENERGY RESEARCH AND PRODUCTION,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, D.C.

The subcommittee met, pursuant to notice, at 9:45 a.m., in room 2318, Rayburn House Office Building, Hon. Mike McCormack (chairman of the subcommittee) presiding.

Mr. McCORMACK. The meeting will come to order, please.

Good morning, ladies and gentlemen.

Today the Subcommittee on Energy Research and Production starts 3 days of hearings on the issue of nuclear powerplant safety.

As we are all aware, this subject has been in the public's mind since the Three Mile Island accident on March 28. However, it is important to note that nuclear safety is not a new issue with this committee or with its predecessor, the Joint Committee on Atomic Energy. It is not a new issue with the Nuclear Regulatory Commission or its predecessor, the Atomic Energy Commission. Indeed, it is not a new issue with the nuclear industry.

The need for strict safety precautions has been recognized since the inception of nuclear power development, and this is borne out, of course, by the excellent safety record of our nuclear powerplants. Not a single person has ever been harmed by any nuclear accident in any nuclear powerplant anywhere in the free world.

However, it is clear that if nuclear energy is to move forward as a major contributing factor in the energy mix of the free world, the questions concerning nuclear safety that are in the public's mind and that have been exaggerated by the Three Mile Island accident must be understood, must be answered, and must be rationalized.

The hearings beginning today are the second in a series of three sets of hearings on nuclear issues which this subcommittee is addressing.

Last week the subcommittee held three hearings on nuclear waste management, and on June 13, 14, and 15 they will hold 3 days of hearings on low-level radiation.

The Three Mile Island accident, focusing our attention on the question of nuclear safety, was clearly a serious accident. There were a number of mechanical failures, possible design weaknesses, and possible operator errors. All these mechanical failure, design weaknesses, and human errors occurring together in a very short time made the accident as serious as it was. However, it was not a catastrophe, and the maximum radiation exposure received by any citizen was at most equivalent to an X-ray.

Similarly, we must remember that this Nation has accumulated about 460 reactor years of experience with licensed commercial nuclear powerplants, and a much larger amount of experience with our naval nuclear reactor program. There are more than 100 licensed nuclear powerplants operating outside the United States in the free world, also contributing to that pool of knowledge and experience.

In all that time, as I say, there has never been a single person harmed, let alone killed, by any nuclear accident in any nuclear powerplant.

I want to emphasize that these hearings today will be broad in scope. We are starting with the basic concepts of nuclear powerplant construction, philosophy, safety, and operation.

The main objective of holding these hearings is to help the committee, and the Congress, and members of the public to understand the questions associated with nuclear powerplant safety. Also, to help the committee and the Congress to take what steps it feels necessary in assuring that our nuclear powerplants will be even safer in the future than they are today.

Learning the lessons from Three Mile Island, asking the tough questions, and providing responsible answers to them will be part of the functioning of this committee.

This committee, by the way, has the responsibility for energy research, development, and demonstration associated with our nuclear powerplant research, development, and demonstration programs which ultimately will lead to commercialization.

In conducting these hearings, the subcommittee intends to explore every aspect of safety technology and to conduct a thorough review of the status of the technology. We want to develop a detailed understanding of nuclear safety and operating philosophy as well as the implications of the Three Mile Island accident and any other accident.

In so doing, we will seek unique perspectives from outside the nuclear energy community itself and, among others, we will hear from Admiral Rickover, to learn his perspectives on providing adequate safety standards for a nuclear system. But today the hearings will concentrate on the philosophy and the status of technology of safety systems and procedures.

Today's hearings will include testimony from the nuclear industry, the Nuclear Regulatory Commission, and a nuclear critic. The Rasmussen report on reactory safety will also be discussed, together with recent criticism of it by the Lewis panel. Tomorrow, witnesses will concentrate on the Three Mile Island accident itself and its technological implications. That testimony will cover industry, utility, regulatory, and State government views of the accident.

We are particularly interested in the system failures and the extent to which human error played a role in the accident.

The final hearings on Thursday will provide additional perspectives on nuclear safety. Representatives of the Swedish nuclear industry will testify about this program, and Admiral Rickover, as I have said, head of the naval nuclear reactor program, and Dr. George Low, former Deputy Administrator of the National Aeronautics and Space Administration, will provide their unique views

on safety systems and methods for improving the interface between men and machines.

Before we move into our testimony this morning, I would like to introduce some distinguished guests that we are honored to have visiting us today. We have with us four Members of the French Parliament, the equivalent of our Congress, and they are seated here to my left, in the front row.

Since I am not very good at speaking French or pronouncing French names, I would like to ask Dr. Pierre Zaleski, the nuclear attaché of the French Embassy, to introduce our guests from the French Parliament.

Dr. Zaleski.

Dr. ZALESKI. Thank you, Mr. McCormack.

We have here a delegation of French Parliament, the head of the delegation on my left is Mr. M. Xavier Hamelin, President, Depute du Rhone, 12eme circonscription—Groupe du Rassemblement pour la Republique; Vice President de la Commission de la Production et des Echanges; Conseiller municipal de la Mulatiere; Ne le 4 fevrier 1922 au Lardin—Dordogne; Ingenieur chimiste; Elu a l'Assemblee Nationale le 11 mars 1973; Reelu le 19 mars 1978.

Membres: M. Roger Couhier, Depute de la Seine-Saint-Denis, 5eme circonscription—Groupe communiste; Marie de Noisy-le-Sec; Ne le 26 janvier 1928 a Vitrai-sous-Laigle—Orne; Employe a la S.N.C.F.; Elu a l'Assemblee Nationale le 12 mars 1967; Reelu les 11 mars 1973 et 19 ars 1978.

M. Paul Pernin, Depute de Paris, 11eme circonscription—Appar-ente au groupe de l'Union pour la Democratie fraçaise; Marie-adjoint de Paris; Ne le 30 octobre 1914 a Oran—Algerie; Conseil d'entreprise; Elu a l'Assemblee Nationale le 19 mars 1978.

M. Allain Chernard, Depute de Loire-Atlantique, 2eme cir-cription—Groupe socialiste; Conseiller general, Marie de Nantes; Ne le 20 fevrier 1937 a Nantes—Loire-Atlantique; Ingenieur; Elu a l'Assemblee Nationale le 19 mars 1978.

Mr. MCCORMACK. Thank you very much.

I think we ought to give our French guests a hand. [Applause.]

May I say for the benefit of the audience that the blonde lady in the middle, who was not introduced, is an interpreter, and since I can't speak French names, I am going to have trouble with that one too. I want to welcome all of you, and say that the representa-tives introduced represent four different French political parties. France has a unified program which provides nuclear leadership throughout the world. Not only are they moving forward agressive-ly with their light-water reactor program, their pressurized-water reactors, but they are also moving forward with the breeder program.

The French Phenix has been on line since 1973 and it is perform-ing beautifully. The Super Phenix is under construction near Lyon. The French are glassifying waste and they are way ahead of the rest of the free world in that. They now have a major uranium enrichment program, and of course a reprocessing program. They are providing leadership for all the free world, and we congratulate them on that, and I want to thank you gentlemen.

Members who left after they were introduced are going to another committee meeting, but they are going as a team, to come here and look at our nuclear program.

Before we begin our testimony I would like to welcome Congressman Goldwater this morning, and I want to ask Mr. Goldwater if he would like to make an opening statement.

Mr. GOLDWATER. Thank you very much, Mr. Chairman.

I join you in welcoming our friends from France. France is a great country, and they are a great people, who I think provide our world with leadership and who have made a significant contribution to mankind, and I think it is a wonderful gesture when Members of the French Parliament come over to exchange ideas and to learn some of the things that we are doing, and hopefully we can learn from them.

I think, Mr. Chairman, these hearings are timely. I think this committee must look carefully at the status of safety technology and related procedures and practices for operating nuclear plants. These hearings should indicate where technology improvements are warranted so that the committee can identify areas for specific program initiatives.

This is a time for frankness. No one can afford to overlook any aspects of safety which can reasonably be enhanced. Although the nuclear safety record has been very impressive, neither the industry nor the utilities can afford to approach nuclear safety with a business as usual view. A serious accident did occur, and we must learn from it.

Today we will learn where the technology is so we can identify specific elements which must be enhanced. Public perception of these issues demands fresh scrutiny of how to plan for likely events. We should not succumb to any temptation to preoccupy ourselves with a series of improbable accidents. The combination of human error and absence of adequate instrumentation played a role in this incident, and we must look carefully at aspects of the man-machine interface.

I believe that our witnesses on the third day will provide unique perspectives from outside of the U.S. civilian nuclear community. From the aerospace aspect, I intend to see that the Three Mile Island becomes the Apollo fire for the nuclear industry. I also believe that we should learn from the naval nuclear propulsion program, which utilizes a most thorough system of training, and checks and balances, to insure that their excellent people are given top quality training.

This is a time for soul searching, Mr. Chairman, for without the nuclear option, this country's energy supply problem will be greatly aggravated.

Thank you, Mr. Chairman.

Mr. McCORMACK. Thank you, Mr. Goldwater.

Before we proceed with our hearings, I am going to make an announcement for the record.

During our hearings last week on high-level nuclear waste management, it became obvious that we are taking too much time with questions and discussions, thus depriving ourselves of the balanced presentation available if all witnesses were to be heard. This is also

unfair to the witnesses, several of whom have come long distances to testify.

I expect that this problem of not having enough time for everyone to ask questions, and to say everything he or she wishes, will become apparent this week as we conduct our hearings on nuclear powerplant safety.

It will be obvious that we have attempted to schedule a large number of expert witnesses to provide the members of the committee with the benefit of testimony from a number of different viewpoints.

In order to make it possible for us to complete our hearings on schedule, it will be necessary for the Chair to sharply restrict the amount of time allowed for questions. Accordingly, the 5-minute rule will be strictly enforced.

In addition, it will not be possible for every member to question every witness. Accordingly, questions of each witness will be structured as follows: After questions by the chairman and the ranking minority member, two members from the majority and one from the minority may question the witness. We will then proceed to the next witness. Then two other members from the majority and one other member from the minority may question that witness. This procedure will be followed until all witnesses have testified and been questioned.

If there is additional time after all witnesses have testified and been questioned, additional questions may be asked of any witness who is still present in the room by any member of the committee. In such a situation the 5-minute rule will still apply, and no member may ask more than one question while another member is requesting an opportunity to question a witness.

I regret the necessity of establishing such a procedure, but without doing so, it will not be possible to obtain the information these witnesses will provide during the time we have available.

I know the members of the committee will agree that this system is as fair and practical as any.

Our first witness today is Dr. Joseph Dietrich, chief scientist of the Advanced Nuclear Systems Department of the Combustion Engineering Co. He will participate in a panel which also includes Mr. Milton Levenson, director of the Nuclear Power Division of the Electric Power Research Institute; Mr. William Kennedy, vice president and director of engineering for the Stone & Webster Engineering Corp.; together with Dr. Chauncey Kepford, director of the Environmental Coalition on Nuclear Power.

We will ask these four gentlemen to each present his testimony, and then we will have questions following the testimony of the four witnesses.

Gentlemen, welcome.

We have your written testimony before us, and without objection, all the written testimony that each of you has submitted will be included in the record at this point, and you will be free to proceed to make your presentation and summarize your remarks as you wish.

Dr. Dietrich, do you wish to proceed?

**STATEMENT OF DR. JOSEPH DIETRICH, CHIEF SCIENTIST,
NUCLEAR POWER SYSTEMS, COMBUSTION ENGINEERING**

Dr. DIETRICH. Thank you, Mr. Chairman.

It is a pleasure to testify before this committee on the subject of nuclear plant safety.

I believe that what I say with respect to safety principles and areas in which safety can be improved is representative of industry thinking, but of course when I speak of what is being done within the industry, I will have to confine my remarks to the activities of my company, Combustion Engineering.

I am afraid that when I prepared my written testimony, I did not have an entirely correct concept, had a little bit the wrong impression of the objective of this day's hearings. I thought that its thrust was directly toward the implications of Three Mile Island, but I understand now that the Three Mile Island subject will be addressed directly tomorrow.

Mr. McCORMACK. Dr. Dietrich, we don't want to deprive you of making any point you want to make, and we don't want to deprive this committee of the benefit of your testimony, so I will not try to restrict you to any degree that reduces your effectiveness and makes you uncomfortable.

Dr. DIETRICH. Thank you.

Today we consider the philosophy and technology of nuclear safety. Nevertheless I think my prepared testimony is pertinent, for we have no reason to question our basic safety approach, that is, the defense in-depth principle which provides not only in-depth safety systems designed to cope with postulated accident sequences, but also safeguards of a more general nature with capabilities for countering the effects of unforeseen sequences.

The general safeguards saved the day at Three Mile Island, and provided the means to protect the public. I believe that the only fruitful reexamination of our safety philosophy and technology must be one based on the Three Mile Island experience, which I think did not invalidate the basic principles or the effectiveness of our technology, but did indicate the need for a certain shift of emphasis.

I am appending to my testimony a list of potential research and development projects which are consistent with the lessons of Three Mile Island, and which we at Combustion Engineering feel are worth assessment for possible Government support.

Each of the projects listed is directed toward a rather specific safety function. Most of these functions are applicable generally to pressurized-water nuclear plants, but their effectiveness, the need for them, and the ease or difficulty of implementing them depend upon overall plant design. We, therefore, believe that, for maximum effectiveness, the examination of specific possibilities such as these should be supplemented by an integrated approach which would not only consider existing and proposed individual safety features but would also reexamine the design approaches used for the plant itself.

Here I am not speaking of the possibility of major changes in plant design concepts but of approaches to detailed design which might have safety benefits.

The objective would be to implement design principles which best serve a threefold purpose:

First, to make less difficult demands on the operator, and to be more forgiving of operator errors through minimization of the frequency of occurrence and speed of development of operational perturbations with potential for hazard;

Second, to increase the effectiveness of safety systems and engineered safeguards, and, to the extent possible, to decrease the complexity of integrating those safety features into the overall plant design; and

Third, without compromising the protection of the public from the most severe postulated accidents, to improve defenses against lesser accidents which may result in substantial financial loss and which erode public confidence even if they produce no substantial public hazard.

We recommend a project with these approaches and objectives which would draw expertise from all appropriate segments of the industry and which would be conducted under the aegis of some organization with the capability of sponsoring intraindustry efforts, such as the American National Standards Institute.

I will now consider directly the specific and generic considerations that have resulted from the Three Mile Island experience. The first lesson to be learned is that we must continue to improve the communication between machine and man, and of course I mean this to apply to the operating phase.

Communication from machine to man comes by way of instrumentation. We know that the Three Mile Island experience suggested certain specific hardware improvements that might be made in the instrumentation area. Although the Combustion Engineering plants are rather different in design from the Three Mile Island plant and would have responded differently to the initiating events, we are currently examining these suggested improvements for feasibility, method, and value. They include:

Positive position indication—that is, open or shut—for critical valves;

Instrumentation for indicating water level in the reactor vessel; and

Improved instruments for detecting significant leakage from the primary system.

Generically, the Three Mile Island experience has suggested the degree of safety could be improved by simplifying the interpretation of instrument readings. With this in mind we are initiating an instrumentation review of the Combustion Engineering plants which addresses the generic problem as well as the specific instrumentation needs suggested by the incident. The review has the following objectives:

Find the most direct and positive ways of indicating those conditions that are crucial to the safety of the plant;

Search out any abnormal conditions under which each particular type of instrument could give readings having a significant difference from the normal one, and correct that; and

Finally, whenever possible, assist the operator in recognizing abnormal conditions quickly by combining information from different instruments automatically—for example, via a computer—in

cases where such information processing would give direct indication of an abnormality.

Let me emphasize that we are proceeding out of a sense of prudence, not of doubt about the safety of our systems instrumentation. Our customers, the public, expect no less of us in light of the Three Mile Island incident. On a related, important subject, additional members of the operating crews must be given greater understanding of the entire plant's behavior and of the physical principles that govern that behavior.

Let me now address the second generic lesson to be learned from Three Mile Island: the need for more attention to generalized safeguards as well as those that deal with prepostulated accident scenarios.

The containment building is such a generalized safeguard, and it certainly proved its value at Three Mile Island. We do not visualize another generalized safeguard of the scope and magnitude of the containment building, but we do see the need to continue to search out the possibilities of hazardous conditions, regardless of how those conditions might come into being, and provide means to cope with them.

The Three Mile Island experience, for example, demonstrated the need for a means of remotely controlled venting of noncondensable gases from the dome of the reactor vessel.

We are undertaking a generic investigation of the need for additional general safeguards equipment.

In conclusion, let me say that the engineering of new safety equipment must proceed on an integrated systems basis to assure that equipment added to improve safety under one set of circumstances does not degrade it under other circumstances.

Finally, let me repeat something our company president, Mr. Arthur Santry, said recently at our annual meeting of shareholders. He said that it is essential that we all heed President Carter's urging to proceed with "care and reason" in considering the effects of the Three Mile Island incident.

Nuclear power is far too important to be written off in an atmosphere of fear, doubt, and incomplete information. I know that you, Mr. Chairman, and the members of your committee are sincerely engaged in a search for truth about nuclear plant safety, and I pledge my full support and that of my colleagues in the Nuclear Power Systems Division of Combustion Engineering to help toward that end.

I thank you very much.

[The prepared statement and biographical sketch of Dr. Dietrich follow:]

Testimony for the Subcommittee on Energy Research and Production
of the U. S. House of Representatives, 5/22/79

I am Joseph R. Dietrich, Chief Scientist for Nuclear Power Systems at Combustion Engineering, Inc., and for many years Chairman of the Nuclear Safety Committee for my company.

It is a pleasure to testify before the Subcommittee on Energy Research and Production, on the subject of nuclear plant safety. I believe that what I say with respect to safety principles and areas in which safety can be improved is representative of industry thinking, but when I speak of what is being done within the industry I am confining my remarks to the activities of Combustion Engineering.

I am sure that a primary concern of this Committee is the implications of the recent incident at Three Mile Island, so I will concentrate on those implications. The Three Mile Island experience is regrettable and very costly, and an experience which we are studying intensively so that our knowledge of safety technology and operating practices may continue to improve.

A nuclear power plant is a complex system of machinery. That is why its designers have adopted the defense-in-depth principle for its safety design. That principle provides not only in-depth safety systems and carefully engineering safeguards designed to cope with postulated accident sequences, but also safeguards of a more general nature with capabilities for countering the effects of unforeseen sequences.

I believe the public is protected by the generalized safeguards. The Three Mile Island incident did not prove otherwise. While the specific accident sequence was unforeseen, the engineered safeguards used were successful in protecting the public.

One generic lesson to be learned from Three Mile Island is that we must continue to improve the communication between machine and man. Another is that we must give increased attention to generalized safeguards, as distinguished from those that deal with pre-postulated accident scenarios. In discussing these points I will cite specific improvements suggested by the Three Mile Island experience, and place them in the context of more generalized classes of possible safety improvements which merit further investigation.

I am also appending to this testimony a list of potential research and development projects which are consistent with the approaches suggested here, and which we at Combustion Engineering feel are worth assessment for possible government support. Some of these have already been discussed with appropriate staff of the Department of Energy.

Each of the projects listed is directed toward a rather specific safety function. Most of these functions are applicable generally to pressurized water nuclear plants, but their effectiveness, the need for them, and the ease or difficulty of implementing them depend upon over-all plant design. We therefore believe that, for maximum effectiveness, the examination of specific possibilities such as these should be supplemented by an integrated approach which would not only consider existing and proposed individual safety features, but would also re-examine the design approaches used for the plant itself. Here I am not speaking of the possibility of major changes in plant design concepts, but of approaches to detailed design which might have safety benefits. The objective would be to implement design principles which best serve a three-fold purpose:

- to make less difficult demands on the operator, and to be more forgiving of operator errors through minimization of the frequency of occurrence and speed of development of operational perturbations with potential for hazard;
- ✓ to increase the effectiveness of safety systems and engineered safeguards, and, to the extent possible, to decrease the complexity of integrating those safety features into the over-all plant design;
- without compromising the protection of the public from the most severe postulated accidents, to improve defenses against lesser accidents which may result in substantial financial loss and which erode public confidence even if they produce no substantial public hazard.

We recommend a project with these approaches and objectives which would draw expertise from all appropriate segments of the industry, and which would be conducted under the aegis of some organization with the capability of sponsoring intra-industry efforts, such as the American National Standards Institute. ✓

Let me now return to the subject of the specific and generic considerations that have resulted from the Three Mile Island experience. I have said earlier that the first lesson is that we must continue to improve the communication between machine and man, and I mean this to apply to the operating phase.

✓ Communication from machine to man comes by way of instrumentation.

We know that the Three Mile Island experience suggested certain specific hardware improvements that might be made in the instrumentation area. Although the Combustion Engineering plants are rather different in design from the Three Mile Island plant, and would have responded differently to the initiating events, we are currently examining these suggested improvements for feasibility, method, and value. They include:

- Positive position indication (i. e. open or shut) for critical valves.
- Instrumentation for indicating water level in the reactor vessel.
- Improved instruments for detecting significant leakage from the primary system.

Concomitantly The Three Mile Island experience has suggested the degree of safety could be improved by simplifying the interpretation of instrument readings. With this in mind we are initiating an instrumentation review of the Combustion Engineering plants which addresses the generic problem as well as the specific instrumentation needs suggested by the incident. The review has the following objectives:

- Find the most direct and positive ways of indicating those conditions that are crucial to the safety of the plant.
- Search out any abnormal conditions under which each particular type of instrument could give readings having a significance different from the normal one. ✓ When such conditions are found, provide other instruments or adequate operator instructions for recognizing the abnormality.
- ✓ Whenever possible, assist the operator in recognizing abnormal conditions quickly by combining information from different instruments automatically (e. g. via a computer) in cases where such information processing would give direct indication of an abnormality.

Let me emphasize that we are proceeding out of a sense of prudence, not of doubt about the safety of our systems' instrumentation. Our customers, the public, expect no less of us in light of the Three Mile Island incident. On a related, important, subject, additional members of the operating crews must be given greater understanding of the entire plant's behavior and of the physical principles that govern that behavior.

Let me now address the second generic lesson to be learned from Three Mile Island: the need for more attention to generalized safeguards as well as those that deal with pre-postulated accident scenarios. The containment building is such a generalized safeguard, and it certainly proved its value at Three Mile Island. We do not visualize another generalized safeguard of the scope and magnitude of the containment building, but we do see the need to continue to search out the possibilities of hazardous conditions, regardless of how those conditions might come into being, and provide means to cope with them. The Three Mile Island experience, for example, demonstrated the need for a means of remotely controlled venting of non-condensable gases from the dome of the reactor vessel. While we do not believe that there was ever a danger from the explosion of the so-called hydrogen bubble, the presence of that non-condensable gas was a major impediment to coolant circulation and pressure reduction during the process of recovery from the incident. A generic investigation of the need for additional general safeguard equipment is being initiated at Combustion Engineering.

✓ In conclusion let me say that the engineering of new safety equipment must proceed on an integrated systems basis to assure that equipment added to improve safety under one set of circumstances does not degrade it under other circumstances.

Finally, let me repeat something our Company president said recently at our annual meeting of shareholders. He said that it is essential that we all heed President Carter's urging to proceed with "care and reason" in considering the effects of the Three Mile Island incident. ✓ Adding to that, let me say, there is no justification, in my opinion, to denigrate the hard work of many talented, dedicated engineers and scientists who literally have devoted their lives to trying to make nuclear power work for the nation's energy needs—with the utmost concern for the safety of our citizens and workers. There also is no justification to automatically condemn as hazardous the nuclear plants that have been operating efficiently and safely for many years before the TMI incident.

I believe you, Congressman McCormack, and the members of your subcommittee are sincerely engaged in a search for truth about nuclear plant safety and I pledge my full support and that of my colleagues in the Nuclear Power Systems Division of Combustion Engineering to help in that end.

Again, as Arthur J. Santry, Jr., Combustion Engineering's president has said, "Nuclear power is far too important to be written off in an atmosphere of fear, doubt and incomplete information".

Thank you for your attention.

List of Suggested R&D Projects

The following is a suggested list of projects for consideration in a government-sponsored safety R&D program. The list contains some that have not yet been thoroughly assessed for their potential value or effectiveness. There is no intent to imply that the developmental products of all of the projects listed are needed for safety improvement; some of the projects represent alternate routes to the same result, and some would simply result in alternate, and possibly better, ways of implementing safety functions already provided on operating plants.

- Improvement of Analytical Methods and Computer Codes
 1. Development of a Best Estimate* NSSS (Nuclear Steam Supply System) Simulation Code for Non-LOCA Design Basis Events
 2. Development and Test of a Best Estimate* Small Break LOCA Model
 3. Development of an Improved Set of Event Scenarios for Consideration During Safety Evaluations
 4. Verification of Methodology of Best Estimate* NSSS Models
 5. Extension of NSSS Simulation Codes to Include the Power Conversion System
- Analytical Investigations
 1. Best Estimate* NSSS and Containment Transient Analysis for Operator Guidance and Training
 2. Evaluations of Changes in Plant Design Features
 3. Natural Circulation Separate Effects Studies and Best Estimate Analysis*

* Analyses and computer codes used for licensing calculations have built-in conservatism which yield conservative results, but distort the calculated course of events relative to reality. Alternate "best estimate" codes are needed to give designers and operators the true picture of the physical situation to be addressed.

4. Analysis of Post-Accident Operation of Reactor Coolant Pump Auxiliaries and Recommendations for Post-Accident Handling of Pumps
 5. Development of Fuel Behavior Analysis System, and Analysis of Methods of Operation for Minimizing Probability of Fuel Damage
 6. Analytical Prediction of Behavior of Reactor Core When Under-Cooled
- Fluid System Improvements
1. Design Development of a High Pressure Shutdown Cooling System
 2. Design Development of a Passive Residual Heat Removal System
 3. Design Development of a Post-Accident Sampling and Chemical Control System
 4. Design Development of a Post-Accident Reactor Coolant System Venting and Degassing System
 5. Evaluation of Radioactive Waste Processing Systems under Post-Accident Conditions
 6. Equipment Certification for Radioactive Waste Treatment Systems under Post-Accident Conditions
- Instrumentation, Control, and Monitoring
1. Development of a Reliable System for Giving Positive Indication of Relief Valve Position
 2. Feasibility Evaluation of Measurement of Reactor Vessel Water Level
 3. Development of a Plant Status Monitoring System
 4. Development of a Display System to Indicate Proximity to Operating Limitations During Off-Normal Conditions
 5. Development of a Display System to Indicate and Predict Trends of Safety-Related Plant Variables
 6. Development of a Post-Accident Plant Monitoring System

- Operating Procedures and Man-Machine Interface
- 1. Develop and Assess Symptom/Function Oriented Operating Procedures for Abnormal Conditions, as an Alternative to Event Oriented Procedures
- 2. Improve and Expand Procedures for Initiating and Maintaining Natural Circulation
- 3. Improve Information Displays through the Application of Human Engineering Principles
- 4. Development of an Advanced Monitoring System to Provide Diagnostic Information, Recommend Corrective Actions, and Pre-Calculate Effects of Specific Operator Actions under Prevailing Conditions

RESUMÉ

JOSEPH R. DIETRICH

Chief Scientist, Nuclear Power Systems, Combustion Engineering, Inc., Ph. D., Physics, University of Virginia, 1939. During the years of World War II worked as a physicist with National Advisory Committee for Aeronautics. Has been in nuclear power development since 1946, joining the first "Power Pile" group at Oak Ridge. Later, at Argonne National Laboratory, was in charge of reactor physics for the prototype power plant for first nuclear submarine. At Argonne was in charge of planning, theory and experimental instrumentation for BORAX experiments, and during 1953 and 1954 was one of team which carried out the experiments at National Reactor Testing Station. These were the first large-scale reactor safety experiments; they demonstrated the inherent safety of the light water moderated nuclear reactor against reactivity accidents, and proved the feasibility of the boiling water reactor.

Later became Associate Director of the Reactor Engineering Division at Argonne. 1956-1964, a Vice President of General Nuclear Engineering Corporation, Dunedin, Florida, which, during the latter part of that period, was a subsidiary of Combustion Engineering. In 1964 became Chief Scientist, Nuclear Power Systems, for Combustion Engineering at Windsor, Connecticut.

His current duties cover line responsibility for advanced systems, including the fast breeder, as well as participation in such over-all technical management activities as R&D direction, coordination of international technical cooperation, and planning and policy decisions.

Compiled and edited (with Dr. Walter H. Zinn) the United States Presentation volume Solid Fuel Reactors for Second International Conference on Peaceful Uses of Atomic Energy in 1958. Was Editor of AEC-published quarterly technical review, Power Reactor Technology from 1961 to 1965. Fellow, and was President of American Nuclear Society for the 1977-1978 term; Member, National Academy of Engineering.

Mr. McCORMACK. Thank you, Dr. Dietrich. We appreciate your statement, and I have some questions for you when the times comes.

I would like to move now to Mr. Milton Levenson.

Mr. Levenson is director of the Nuclear Power Division of the Electric Power Research Institute. EPRI is doing a great deal of research on its own, and it has been doing so for a long time.

We are very pleased to have you here, Milt, and we would like to ask you to proceed with your testimony as you wish.

STATEMENT OF MILTON LEVENSON, DIRECTOR, NUCLEAR POWER DIVISION, ELECTRIC POWER RESEARCH INSTITUTE

Mr. LEVENSON. Thank you.

Mr. Chairman, members of the committee and distinguished guests, my name is Milton Levenson. I am director of the Nuclear Power Division of the Electric Power Research Institute.

I recently served as chairman of the Three Mile Island Ad Hoc Industry Advisory Group, a group of 100 experts from all sectors of the technical community, including reactor manufacturers, architect/engineers, utilities, national laboratories, universities, consult-

ants, NASA, and EPRI. This group responded to the call for help issued by GPU, and provided an independent onsite review of all major actions undertaken during the month following the TMI accident. The basis of my remarks is this recent experience superimposed on a background of 35 years in nuclear R. & D.

The aspect of today's hearing theme of "Nuclear Reactor Safety Systems—Philosophy and Technology" that I would like to comment on is the man-machine interface.

Dr. Dietrich has mentioned that phrase. One member, Mr. Goldwater, also mentioned that phrase. It is clearly an important part of the issue, but I think it is not just the classical question of what should be done by a man or what should be done by the machine, but I think we must address the much broader issues of man's relation to the machine, not only the man in the control room, but during design, construction, management, all aspects of operation, including maintenance, and regulation.

The TMI accident was very serious from a plant damage standpoint, and involved a very complex chain of events whose succession after the originating event was triggered by both men and machines. Because of the complex nature of both the systems and the accident, it will be some time before all the lessons that can be learned are learned. In fact, a significant number of the lessons—my personal opinion is the majority of the lessons—will have nothing to do with the accident itself but will be learned because the system is being subjected to a scrutiny considerably more intense and somewhat different in direction than has been the case in the recent past.

During the weeks spent at Harrisburg and in the weeks since, I have been attempting to categorize, both the initiating events and the secondary events—not only from the overall safety aspects concerning what should we do about running plants, but also from the viewpoint of on the nuclear R. & D. program for which EPRI is responsible.

I have been unable to identify any new phenomena uncovered by the accident, nor have there really been any major surprises to the technical or scientific community with the exception, and it is perhaps a very large exception, of the realization of how preoccupied everyone had become with an unlikely public catastrophe—TMI was not such a catastrophe.

I am sure that the current scrutiny nuclear plants are undergoing will lead to some changes in the nuclear steam supply system hardware, some changes in the balance of plant, some revision in the roles and emphasis of supervision and management, some revisions in operations including information display and analysis. It will probably also lead to revisions in the emphasis of training programs and procedures and to changes in regulation.

These changes will not require extensive new developments nor research into entirely new areas nor require new technology, but rather will require that we go back into more mundane areas we once explored more thoroughly, but in recent years have skimmed over in our search for larger and more serious pseudo-hazards with which to terrify ourselves. Designing and building powerplants so that they have a minimum probability of failing under improbable events does not guarantee maximum safety and does not guarantee

that the risk to the public is at the practically achievable minimum. It is much more important to design and protect against events which are more likely to occur.

Training operators to respond to accidents initiated by double ended, guillotine, large pipe breaks, coincident with either a large earthquake or a large commercial airliner crashing into the plant does not necessarily train that operator to properly cope with a stuck valve or an ambiguous water level indication, and more intense training is no answer if the training is for the wrong contingency.

Risk assessments have been done by many groups in this country and several are underway abroad. I don't intend to get into the argument of the merits of any particular study nor defend the absolute values of any of the conclusions, but I think there is one thing that is consistent in all of the studies and I think is defensible, and that is the maximum risk arises not from the maximum events, but rather from the aggregate of the lesser events.

The message of Three Mile Island is that we must go back and assure ourselves that we are doing everything that is practical to reduce the risk to the public and to the plant, instead of attempting to assure ourselves that we are doing everything possible about the largest conceivable accidents.

To do this, we must review our plant designs. We must ask ourselves how we operate our plants and how we manage them and how we regulate them when lesser accidents occur so that another TMI sump pump out doesn't occur.

We must refocus the thinking of the designers, the builders, the owners, the operators, and the regulators toward this objective of minimizing the real risks. It is essential that this be a common objective because if it is not also the objective of the reviewers and regulators, it becomes an unachievable goal.

The theme of today's session is "Safety Systems," and we all recognize that both men and machines are essential parts of that system. I believe that safety enhancement will be maximized by remembering that it isn't only the operator and the switch he throws, but also the designer and the lines he draws, the electrician and the wires he pulls, and the regulator and the changes he permits or induces or in some cases demands. Each of these actions can be done correctly and each can be done incorrectly, and therefore, reviews of checks and balances must exist for all.

It should be noted that while TMI was a very serious accident from the property damage standpoint and from its financial impact, and we should recognize that the financial impact is due primarily to the high price of the replacement electricity produced from oil compared to the cheaper cost of nuclear power, and it may have been a disaster from the communications standpoint, it was not a disaster from the public safety standpoint.

Because many of the lessons learned have already been implemented, those nuclear plants now operating are even safer than they were before the accident.

In closing, I would like to say that I think it would be unfortunate indeed if TMI resulted in massive new programs to explore extremely unlikely events, or at the other extreme, people attempt to gloss it over by saying, it is just better operator training is all we need, or better management. It was a system problem. I think we must review all aspects of this system and improve each and every piece of the total system.

Thank you, Mr. Chairman.

[The prepared statement and biographical sketch of Mr. Levenson follow:]

MILTON LEVENSON

Milton Levenson is Director of the Nuclear Power Division, Electric Power Research Institute (EPRI), Palo Alto, California.

Prior to joining EPRI, Levenson was Associate Laboratory Director for Energy and Environment at the Argonne National Laboratory in Argonne, Illinois.

At Argonne he at various times held the positions of project manager of the Argonne Advanced Research Reactor, Project Director of the Experimental Breeder Reactor, and Deputy Director of the Chemical Engineering Division.

Prior to joining Argonne, Mr. Levenson worked at what is now the Oak Ridge National Laboratory from 1944 to 1948.

Levenson was chairman of Argonne's Reactor Safety Review Committee from 1954 to 1968 and was technical advisor at the Geneva Conferences on the Peaceful Uses of Atomic Energy in 1958, 1964, and 1971.

Levenson is a member of the National Academy of Engineering, a Fellow of the American Nuclear Society, and a member of the American Institute of Chemical Engineers as well as the recipient of its Robert E. Wilson Award for 1975.

TESTIMONY FOR THE HOUSE SUBCOMMITTEE ON

ENERGY RESEARCH AND PRODUCTION

BY

MILTON LEVENSON

MAY 22, 1979

Electric Power Research Institute
P. O. Box 10412
Palo Alto, CA 94303
415/855-2030

Testimony for the House Subcommittee on
Energy Research and Production

by

Milton Levenson

May 22, 1979

Mr. Chairman, members of the committee, my name is Milton Levenson. I am Director of the Nuclear Power Division of the Electric Power Research Institute.* I recently served as Chairman of the Three Mile Island Ad Hoc Industry Advisory Group, a group of 100 experts from all sectors of the technical community including reactor vendors, architect/engineers, utilities, National Laboratories, universities, consultants, NASA and EPRI. This group responded to the call for help and provided an independent on-site review of all major actions undertaken during the month following the TMI accident. The basis of these remarks is this most recent experience superimposed on a background of 35 years in nuclear R & D.

The aspect of today's hearing theme of Nuclear Reactor Safety Systems - Philosophy and Technology that I would like to comment on is the man-machine interface - not just the classical question of what should be done by a man and what should be automated, but rather the much broader issues of man's relation to the machine during design, construction, management, operation, and regulation. The TMI accident was very serious from a plant damage standpoint, and involved a very complex chain of events whose succession was triggered by both men and machines. Because of the complex nature of both the systems and the accident, it will be sometime before all the lessons that can be learned are learned and, in fact,

* EPRI is a not-for-profit research institute established by the electric utility industry to manage research leading toward low cost, yet reliable electric power. The membership consists of government, municipal, rural cooperative and investor-owned utilities. Approximately one-quarter of the budget is related to research in the nuclear power area, about 30 is devoted to fossil fuel research, and there are ongoing programs in all relevant areas of electric power research.

a significant number of the lessons will have nothing to do with the accident, but will be learned because the system is being subjected to a scrutiny considerably more intense than has been the case in the recent past.

During the weeks spent at Harrisburg and in the weeks since, we have been attempting to categorize both the initiating events and the secondary events - not only from the overall safety aspects, but also from the viewpoint of impact on the Nuclear R & D Program that EPRI is responsible for. We have been unable to identify any new phenomena uncovered by the accident, nor have there really been any major surprises to the technical or scientific community except for the realization of how preoccupied everyone had become with the unlikely public catastrophe.

I am sure that the current scrutiny will eventually lead to some changes in the Nuclear Steam Supply System Hardware, to some changes in the Balance of Plant Hardware, to some revision in the roles and emphasis of supervision and management, to some revisions in operations including information display and analysis and revisions in the emphasis of training programs and procedures and also to changes in regulation. These changes will not require extensive new developments nor research into entirely new areas nor require new technology, but rather will require that we go back into more mundane areas we once explored more thoroughly, but in recent years have skimmed over in our search for larger and more serious hazards with which to terrify ourselves. Designing and building power plants so that they have a minimum probability of failing under improbable events does not guarantee maximum safety and does not guarantee that the risk to the public is at the practically achievable minimum. It is more important to design and protect against the more likely.

Training operators to respond to accidents initiated by double ended guillotine large pipe breaks coincident with either a large earthquake or a large commercial airliner crashing into the plant does not necessarily train that operator to properly cope with a stuck valve or an ambiguous water level indication. Risk assessments have been done by many groups in this country and several are underway abroad. I don't intend to argue the merits of any particular study nor defend the absolute values of any of the conclusions, but one thing the studies all point out is that the maximum risk arises not from the maximum events, but rather from the aggregate of the lessor events.

The confirmatory message of Three Mile Island is that we must go back and assure ourselves that we are doing everything that is practical to reduce the risk to the public and to the plant, instead of attempting to assure ourselves that we are doing everything possible about the largest conceivable accidents. To do this, we must review our designs and plants for lessor events - for example, to make sure that containment buildings isolate on lessor accidents so that another TMI sump pump-out doesn't occur automatically. We must refocus the thinking of the designers, the builders, the owners, the operators and the regulators toward this objective of minimizing real risks. It is essential that this be a common objective, because if it is not also the objective of the reviewers and regulators, it becomes an unachievable goal.

The theme of today's session is Safety Systems, and we all recognize that both men and machines are essential parts of that system. I believe that safety enhancement will be maximized by remembering that it isn't only the operator and the switch he throws, but rather also the designer and the lines he draws, the electrician and the wires he pulls, and the regulator and the changes

he permits or induces or demands. Each of these actions can be done correctly and each can be done incorrectly and, therefore, reviews of checks and balances must exist for all.

It should be noted that while TMI was a very serious accident from the property damage standpoint and from its financial impact - due primarily to the high price of the replacement electricity produced from oil compared to nuclear - and it may have been a disaster from the communication standpoint, it was not a disaster from the public health standpoint.

Because many of the lessons learned have already been implemented; those nuclear plants now operating are even safer than they were before the accident.

In closing, I would like to say that I think it would be unfortunate indeed if TMI resulted in massive new programs to explore the unlikely or, at the other extreme, resulted in people oversimplifying the cause and saying we just need different management or better operators or more training will solve it all. It was a system problem, and we must address it as such.

MILTON LEVENSON

Milton Levenson is Director of the Nuclear Power Division, Electric Power Research Institute (EPRI), Palo Alto, California.

Prior to joining EPRI, Levenson was Associate Laboratory Director for Energy and Environment at the Argonne National Laboratory in Argonne, Illinois.

At Argonne he at various times held the positions of project manager of the Argonne Advanced Research Reactor, Project Director of the Experimental Breeder Reactor, and Deputy Director of the Chemical Engineering Division.

Prior to joining Argonne, Mr. Levenson worked at what is now the Oak Ridge National Laboratory from 1944 to 1948.

Levenson was chairman of Argonne's Reactor Safety Review Committee from 1954 to 1968 and was technical advisor at the Geneva Conferences on the Peaceful Uses of Atomic Energy in 1958, 1964, and 1971.

Levenson is a member of the National Academy of Engineering, a Fellow of the American Nuclear Society, and a member of the American Institute of Chemical Engineers as well as the recipient of its Robert E. Wilson Award for 1975.

Mr. McCORMACK. Thank you, Mr. Levenson.

We also have some questions for you when the time comes.

Our next witness is Mr. William Kennedy, vice president and director of engineering, Stone & Webster Engineering Corp.

Mr. Kennedy, you are welcome. We have your testimony in its entirety, and it will be included in the record, and we should like to have you proceed as you wish.

STATEMENT OF WILLIAM KENNEDY, VICE PRESIDENT AND DIRECTOR OF ENGINEERING, STONE & WEBSTER ENGINEERING CORP.

Mr. KENNEDY. Thank you very much, Mr. Chairman.

I will summarize my testimony, and probably throw in a few more thoughts.

My name is Bill Kennedy, vice president and director of engineering of Stone & Webster.

Not only am I responsible for our nuclear work, but I do a great deal in fusion, solar, and all kinds of other things.

Mr. McCORMACK. I am going to have to ask you to speak a little harder into that mike. You have to drive these mikes pretty hard.

Mr. KENNEDY. I am glad to appear before the committee today to offer some general thoughts on a part of the engineering profession in the nuclear industry.

Safety, it is fundamental to an engineer's philosophy. We have in nuclear industry probably misled the public in that we have allowed ourselves to concentrate on major accidents with extremely low probability, and in that way we have allowed the public to believe that we thought and told them we could design foolproof systems. We cannot nor do we need to.

All of the accidents with which I am familiar in some detail, and I will not comment on Three Mile Island greatly because I have had tremendous difficulty in trying to sort out the facts from fiction, but from Fermi 1 on, in no case was this the kind of an accident on which we had spent the majority of our time. They were much smaller accidents. Certainly they had tremendous economic impact, but none of these accidents represented a clear danger to the public.

The public, however, is left with the impression that we have said that it couldn't happen. Well, what we said couldn't happen didn't in fact happen. We have spent far too much time worrying about these major accidents, a double ended rupture of 3½ inch thick wall pipe, and we have not spent enough time looking at the reliability of lesser important systems.

As engineers, we assume that there will be failures of equipment, operators, and designs, and our designs take this into consideration by the use of redundancy and diversity in these, and as a matter of fact, the nuclear reactor is a pretty important giving device. The plant itself at Three Mile Island and at Fermi before it, the reactor portion of the plant performed very well.

Good engineering then does not assume nothing can go wrong. In fact it assumes precisely the opposite and tries to take account of that.

I have brought along with me a scale model over there which the committee may find of some interest in looking at some of the details regarding safety systems and defense in depth, and I will not dwell on that.

Mr. GOLDWATER. Mr. Kennedy, I am having a difficult time hearing you.

Mr. KENNEDY. I will have to try speaking louder then.

The next two points that I would like to address are quality assurance and standardization, and I can't help note our French friends here. Some of my associates had the privilege of visiting

Gravelines not so long ago. Plants are built in 5 years and on a continuous basis. One of the major difficulties with our quality control requirements in the United States is the fact that the industry is starting and stopping. Our construction workers can and will do a good job. They are interested in quality, particularly they understand the importance of it. Yet all of the changes and all of the time delays that we put into our designs are very debilitating. There is nothing that hurts a workman worse than to see his work removed because somebody decided it needed to be a little bit different. It is a terrible thing on workmen, and pretty quickly they lose interest.

Also, when jobs are started and stopped, it is very hard for them to believe that it is really necessary.

As far as standardization is concerned, I am personally convinced that once again we have referred in large measure to the major accident, whereas it is the detailed engineering that will make this industry go. It is attention to detail.

Just to give you some indication, I worked and was project engineer on the Connecticut Yankee plant, of which I am extremely proud. We spend right now in the design portion for great earthquakes more than the entire engineering that we put in the Connecticut Yankee plant. I personally think that is a complete and total waste. We should be looking at the system design and not wasting our time looking at these very unusual accidents in the depth that we are.

Now I believe the standardization can particularly allow us to get ahead with designs that will in fact withstand major earthquakes, and I note in passing that there is no instance of a modern powerplant being damaged by an earthquake anywhere in the world, and we spend unbelievable amounts of engineering time in doing seismic analysis. But standardization, allows engineers to look at the things we need to, the regulators to look at the things that they need to, and the operators not to have a diversity of plants in which to operate, and when an accident does occur, that there will be many more people much more familiar with the plant.

Certainly the recent accident at Three Mile Island is of great interest to all of us. It is certainly a laboratory waiting to be analyzed. We fairly recently, in Stone & Webster, have taken up using Bell Telephone System PhonoVision for meetings and conferences. My own personal opinion is that one of the things that is missing from our nuclear plants is a much more improved communications system, the use of television, the use of small microphones within containment.

Just think of how nice it would have been to have had two or three TV cameras within the Three Mile Island containment, or even a couple of microphones. I think that this kind of thing can be done. I think our public relations is a problem we didn't think about, that there is absolutely no reason why full information from a faulted powerplant cannot be put into load dispatch centers, almost anything that is necessary so that the operator can virtually instantaneously have at his services the help of some very experienced people.

In short, I believe that the engineering profession has done an outstanding job in designing nuclear powerplants. We have never said they will be foolproof. We will probably have problems again.

We believe that with the proper emphasis on the detailed design, rather than on major accidents, on standardization, and on careful attention to quality control, we will continue to have an excellent and outstanding industry.

Thank you, sir.

[The prepared statement of Mr. Kennedy follows:]

STATEMENT OF WILLIAM J. L. KENNEDY, VICE PRESIDENT AND DIRECTOR TO
ENGINEERING, STONE & WEBSTER ENGINEERING CORP.

Mr. Chairman and members of the subcommittee, My name is William J. L. Kennedy and I am a Vice President and Director of Engineering of Stone & Webster Engineering Corporation.

I am pleased to appear before your subcommittee to discuss nuclear power plant safety philosophy and technology. Stone & Webster has been involved in the design and construction of nuclear energy facilities since the outset of the commercial nuclear power industry, having engineered and built the first demonstration plant, Shippingport.

Needless to say, safety considerations are fundamental to engineering philosophy. Indeed, by definition an engineer's job is to employ technology for the benefit of man in a safe and economical manner. This underlying principle is even more emphasized in the nuclear power field, given the origin of this energy source. Unfortunately, this background has led the public to fear any accident or failure of equipment in a nuclear plant and to assume that any accident in a nuclear plant will have catastrophic effects. Perhaps by way of excessive response to this situation, industry and government alike, through efforts to allay public anxiety, relied so heavily on probability data showing the low likelihood of an accident with severe public consequences that we led the public to believe the nuclear plants are foolproof. Thus, the assertions since TMI that the public was lied to—that "they said it couldn't happen, but it did."

What was said in engineering language was that a major loss-of-coolant accident with a total core melt-down was an event of very low probability; and it did not happen at TMI.

From the outset, an architect-engineer incorporates the philosophy of safety into the basic plant engineering and, in addition, provides specific protection by incorporating redundant safety systems to accommodate possible accident conditions, by separating physically three systems, by adding diverse systems to perform similar functions and by separating safety systems from non-safety systems. The concept is then carried to the extreme of assuming the failure of such systems and providing means to mitigate the results which could be expected. Thus, we add the containment with attendant filtering systems, etc.

We have available a scale model of our reference nuclear plant depicting the various special safety systems employed. I have attached as an appendix to my testimony a listing of the safety features displayed and I'd be pleased to explain them using them the model, as time permits.

This model illustrates the overall "defense-in-depth" reactor safety philosophy used in the design of nuclear facilities. These facilities are designed to provide (1) a large margin of safety for defects in materials and equipment, acts of nature, and possible human error; (2) backup systems that will compensate automatically for failure of essential equipment and (3) equipment and systems (such as the emergency core cooling systems and containment) to limit the public consequences of even highly unlikely accidents.

Application of the "defense-in-depth" philosophy results in the provision of multiple physical barriers between the reactor fuel and the environment outside its plant. The fuel is contained in a sealed metal cladding the clad fuel is contained in a heavy steel primary contain system; and the primary coolant system is enclosed in a massive concrete and steel containment building.

A Quality Assurance program is employed from the outset of the design phase through component manufacture and containment to ensure a finished product of high quality. This program also features multiple, redundant efforts to review calculations, designs, and specifications by independent reviewers. Manufacturers inspect their products and these are verified by both the utilities and AEC. The federal government, through AEC, audits and inspects to ensure program validity.

Obviously, however, quality must be designed and built in at the outset; no amount of inspection will add quality.

QA organizations are independent of production and are answerable directly to top management. This ensures against diminution of QA efforts due to production demands and pressures and enhances objectivity where these interests may conflict.

In the construction of a plant, we have learned that standardization pays handsome dividends. Detailed work processes involving parallel paths and repetitive operations yield a higher degree of skills and therefore improved quality. Our construction innovations program is aimed at using the best and most efficient methods and needs, reducing peak manpower requirements and permitting firmer quality control.

Our basic plant designs are evaluated for safe constructurability, operability, and maintainability. For each phase of a project, we have standardized our construction methods and procedures, such as material controls, handling and storage, steel erection, concrete placement, etc., including independent inspection of each. Special training is provided to responsible personnel on these procedures.

We also have developed a standardized system for reviewing significant engineering, design, construction and QA issue that arise in order to ensure incorporation of lessons learned from each into other project efforts. These efforts, while not unknown to other large industrial programs, are unprecedented in the degree to which they are employed on nuclear facilities. Obviously, the unmatched safety record of the nuclear industry bears witness to the wisdom of this approach.

We believe standardization can contribute positively in a number of ways. Repeated designs and construction and manufacturing techniques and procedures permit increased efficiency resulting in higher quality; and that translates to greater safety. Another significant advantage of standardization in the reduction in the number of plant design variations with which plant operators and emergency teams would have to be familiar. This would concern increased operator capability. Standardization will permit greater concentration of specialized talents on more detailed safety considerations. Standardization will lead to increased efficiency and thus improved safety and, because of favorable cost impact, the additional benefit of lower power costs to the public.

The recent accident at Three Mile Island Unit 2 provides a here-to-fore unavailable perspective from which to view this approach to safety. The defense-in-depth concept appears to be valid. Safety systems did work. The physical integrity of the reactor coolant system was maintained. When initiated, containment was maintained. While we have not had the opportunity to evaluate the data in detail, it appears that this was true despite some failures of equipment and some yet to be explained operator actions. This, I think, demonstrates the remarkable resiliency of the plant to withstand adverse conditions, and that is exactly what is designed to do.

We have much to learn from this event as the detailed information becomes available. The plant has been characterized as a laboratory awaiting analysis and I agree. There are some lessons which are already apparent. Perhaps the most obvious is that in both licensing and design, the industry and the regulators may have been concentrating too hard on the hypothetical catastrophic event involving total instantaneous loss of coolant with the necessity of response in fractions of a second to the exclusion of more likely incidents of lesser severity. I would point out, contrary to what one might believe from reading the papers or watching television accounts, that TMI was far short of such a hypothetical event.

It appears that there is considerable room for improvement in the manner in which information for plant status is made available to the operators and the public. The ability to verify what is actually occurring is vitally important to ensure confident decision making. In this regard, I personally favor extensive use of video and audio relay systems so the plant operators can actually see and hear what is happening. Had the TMI operators seen the water running out of the pressurizer and accumulating on the containment building floor, they obviously would have had a better basis upon which to assess conditions and determine the required responses.

Recent experiments at the LOFT facility in Idaho have confirmed the efficacy of current designs to protect the core against the catastrophic loss-of-coolant accident. The real life experience of TMI indicates the need to expend further effort to ensure that lesser events are not permitted to propagate to endanger the public or plant performance. There are obviously several facets to this including equipment design, control design, and operator training. The safety record of nuclear plants is unmatched by any other industrial sector, and I include recent events in that assessment. We are proud of this record and will strive to improve on it. Of course, the broader aspects of governmental response to emergency conditions and all that involves has been shown to be amenable to improvements as well.

I shall be pleased to respond to your questions.

APPENDIX—SAFETY FEATURES, STONE & WEBSTER MODEL

- Reactor Vessel—Contains core, control rods, and reactor coolant.
- Reactor Core—Generates heat by nuclear fission.
- Reactor Coolant Pumps and Piping System—Circulate reactor coolant.
- Pressurizer—Pressurizes reactor coolant to 2250 psi.
- Pressurizer Relief Tank—Receives pressurizer discharges.
- Steam Generators—Generate non-radioactive steam.
- Reactor Containment and Liner—Contain radioactive vapors.
- Accumulators—Automatically inject emergency core cooling (ECC) water.
- Safety Injection Pumps—Automatically pump ECC water.
- Charging Pumps—Automatically pump ECC water.
- Boron Injection Tank—Boron prevents nuclear chain reaction.
- Residual Heat Removal Pumps—Automatically pump ECC water.
- Residual Heat Removal Heat Exchangers—Remove heat from core.
- Containment Spray Pumps and Spray Headers—Spray reduces pressure and adsorbs radioactive iodine.
- Refueling Water Storage Tank—Stores ECC and spray water.
- Chemical Addition Tank—Adds iodine absorbent to spray.
- Containment Atmosphere Recirculation Coolers—Remove heat.
- Supplementary Leak Collection and Release System Fans and Charcoal Filters—Filter air.
- Hydrogen Recombiner—Removes hydrogen from containment.
- Turbine and Motor Driven Auxiliary Feedwater Pumps—Provide water to steam generators to cool core.
- Auxiliary Feedwater Storage Tank.
- Main Feedwater Piping—From main feedwater pumps.
- Main Steam Piping—To turbine-generator.
- Atmospheric Dump Valves—Release non-radioactive steam to remove heat.
- Containment Isolation Valves—Automatically close when required.
- Cable Trays—Separate red, white, blue, and yellow electrical safety circuits and black non-safety circuits.
- Cable Spreading Areas—Separate cables for protection.
- Control Room.
- Main Control Boards—Used during normal operation.
- Engineered Safety Features (ESF) Control Boards—Control and monitor safety systems.
- ESF Relay, Logic and Actuation Panels—Redundant Safety control equipment.
- Electrical Circuit Breakers—Control and power safety electrical equipment.
- Auxiliary Shutdown Panels—Alternate shutdown controls.
- Batteries—Power safety electrical circuits if off-site power is lost.
- Diesel Generators—Provide standby power if off-site power is lost.
- Fire Protection—Red piping and hose stations.
- Fuel Transfer Mechanism.
- Spent Fuel Racks—Provide underwater storage.
- Spent Fuel Shipping Cask.

Mr. McCORMACK. Thank you, sir. We will come back to the questions presently.

We will now hear from Dr. Chauncey Kepford, director of the Environmental Coalition on Nuclear Power.

Dr. Kepford, welcome. Your testimony will be included in the record. You may proceed

STATEMENT OF DR. CHAUNCEY KEPFORD, DIRECTOR,
ENVIRONMENTAL COALITION ON NUCLEAR POWER

Dr. KEPFORD. Thank you, Mr. Chairman.

First off, I am not the director of the Environmental Coalition on Nuclear Power. One of the codirectors is here with me today, Dr. Judith Johnsrud. By default, I am the legal and technical director of the coalition, because nobody wants to be.

Mr. McCORMACK. We welcome you with whatever title.

Dr. KEPFORD. Thank you.

I wasn't inside at Three Mile Island. I was on the outside. Our house was used and our facilities were used by the refugees from Three Mile Island, people who had to flee their own homes because of this accident, because they were not being told the truth by Metropolitan Edison Co., or the Nuclear Regulatory Commission, about what was going on.

There were thousands of people in this very kind of a position, that they had to leave their homes. It really bothers me to hear this put down as a nasty accident that really didn't hurt anybody, that nobody is going to die from it.

I think such talk is utter bunk and should be described as such. I might add that I am not speaking now from ignorance. I have reviewed quite thoroughly the data contained in the population dose and health impact of the accident at the Three Mile Island nuclear station from the Ad Hoc Population Dose Assessment Group.

I think the review of that data and the monitoring efforts that took place around that accident border on the criminally negligent.

It just happens to turn out that there were no radiation monitors between the plant and the largest concentrations of people. Nor did they go out anywhere near far enough.

The NRC's monitors went out only 13.8 miles. On the basis of a very poor set of data, these gentlemen then dragged out of the sky, out of a hat, a distance-dose model to calculate doses out to 50 miles.

But that model is not supported by the data close in. Why should it be supported farther out? If you would like more details on this, I can give them to you.

With regard to the research philosophy, which is the subject of these hearings, it has been my impression throughout the nuclear power program that the primary emphasis has been based on theoretical impressions of safety rather than experimentally determining safety.

I have characterized this in my testimony as the law of the universe according to Walt Disney: Wishing will make it so.

Let's look at the situation realistically.

Experiments tell us where we are. They give us information that can tell us yes or no, we can go ahead, we should not go ahead. Theoretical calculations, no matter how well founded or what kind of a data base we have, normally have to be treated with suspicion.

For instance, we have 20 years or so of tracking satellites from the satellite program. There are thousands of chunks of metal up there that are monitored more or less on a daily basis.

Yet, now we are facing the fact that Skylab is going to come slipping down on us sometime, perhaps this fall. We cannot predict when. We might have a 20-minute warning. But not to worry because it will happen in somebody else's backyard.

I have been lulled into this false sense of security about nuclear reactors, until Three Mile Island happened in my backyard. I think it is time we stopped delving into this world of theoretical safety, imaginary safety, or speculative safety, or whatever you want to call it, and started going back to the basics, and started asking the question are we at the point where we can prevent the worst imaginable accident; not the design basis accidents that we have

heard about this morning, or maximum credible accident, or hypothetical accident, or postulated accident, whatever?

Do we know that we can prevent a severe power excursion at a nuclear powerplant? I suggest the answer is no.

Do we know that the emergency core cooling system will work as it is designed to? I suggest the answer is no.

Do we know whether or not the ECCS system will work on a hot core? I suggest the answer is no.

Do we even know what happened at Three Mile Island inside that pressure vessel between 4 a.m. Wednesday morning, March 28 and, say, 8 or 10 p.m. March 28? I suggest the answer is no, and it really bothers me that the NRC is rushing forth and slapping a bunch of band-aids on the other operating B and W reactors, and hoping that those band-aids will prevent TMI-2 from happening all over again.

What we don't know, of course, is whether or not those band-aids that the NRC is slapping on will make matters worse. That we don't know.

An interesting question to ask throughout all this is what would have happened if that reactor had failed to scram. One problem that has been nagging the regulatory bodies and the industry for years has been this problem of an anticipated transient without scram; that is, without the reactor shutting down.

The feed water pumps quit at 4 a.m. Wednesday morning. Within 1 minute and 45 seconds after they quit, the reactor had been shut down for virtually all of that time, but in that time, the steam generators boiled dry, and then things started getting sticky.

Of course, they were complicated by the fact that the emergency feed water pumps were turned off. But suppose the reactor hadn't scrambled. Would there be anybody living in eastern Pennsylvania today?

I suggest things might have turned out quite a bit differently. But we don't know, do we? Most of our safety estimations are based on unverified computer calculations. We have an enormous theoretical basis for safety. I suggest our experimental basis for safety is much, much shallower; in fact, dangerously shallow.

I would like to point out some ideas that were communicated to the Joint Committee on Atomic Energy years ago by Dr. Clifford Beck as a result of the results of the steering committee that was working toward revising the original WASH-740. It is just half a dozen lines.

He stated, and this is a letter dated May 18, 1965:

There is no objective, quantitative means of assurance that all possible paths leading to catastrophe have been recognized and safeguarded or that the safeguard will in every case function as intended when needed.

Here is encountered the most baffling and insoluble enigma existing in our technology. It is in principle easy and straightforward to calculate potential damages that might be realized under such postulated accident conditions. There is not even in principle an objective and quantitative method of calculating probability or improbability of accidents or the likelihood that potential hazards will or will not be realized.

I suggest nothing that came out of the reactor safety study contradicts a word that Dr. Beck said. He was talking, after all, about objective and quantitative means of calculating probabilities.

Last, if the theoretical aspects of safety are so good, I suggest that a good method of verifying our predictive abilities will be for elections for Congress, for instance, to be determined on the basis of predicted popularities and so on, say the day before the election, and that all parties agree to the results and postpone the election because the election is, of course, expensive.

That would simplify things. But I don't really think that most Members of Congress would really buy that. They would rather go through the experiment and have it verified.

As one of those who is under the gun, I, too, would like to have the reactor safety experiments verified. Most haven't been. Most are still waiting to be done.

I suggest that those of you who are very dedicated to the furthering of this industry, which has the potential for doing so much damage, and causing such an overwhelming level of human misery, volunteer your districts for the next nuclear success story; that is, an accident which wasn't an accident.

Thank you.

[The prepared statement of Dr. Kepford follows:]

Testimony
of
Dr. Chauncey Kepford
Environmental Coalition on Nuclear Power
before the
Subcommittee on Energy Research and Production
of the
Committee on Science and Technology
May 22, 1979

Mr. Chairman, members of this Subcommittee, it is an honor to appear before this body to discuss the most important subject of nuclear reactor safety today. The near catastrophe at Three Mile Island, Unit 2 has shocked many people on both sides of the ongoing debate about nuclear power. For my own part, I was one of those who had been lulled into believing the soothing chorus of assurances of the promoters of nuclear power, from the Nuclear Regulatory Commission (NRC) on down to the public relations persons for our own local nuclear utilities. This false sense of security fell in face of the recent partial renunciation of the widely and justifiably criticized, (but yet much relied upon) Reactor Safety Study, WASH-1400, or the Rasmussen Report, or Whitewash-1400, as it has been referred to. On top of this, there was the additional, and somewhat sick, rationalization of "safety," and that is that when a serious accident finally does happen, it will be in someone else's backyard.

But things don't always go according to plan. When this "worst yet" nuclear reactor accident did happen, it was in my backyard. It occurred at the very reactor that I had fought throughout its still uncompleted licensing proceeding. In this proceeding, with the most able assistance of Dr. Judith Johnsrud, who is Co-Director of the Environmental Coalition on Nuclear Power, we became aware through our own totally unschooled efforts at cross-examination, that the emergency plans of Dauphin County, where TMI-2 is located,

the Commonwealth of Pennsylvania, and the NRC itself, had no basis in fact at all. Assurances of preparedness were rhetorical only. We did not have the resources to rebut this concept of paper, or even imaginary, preparedness. Subsequent events have thoroughly confirmed our belief that all talk of emergency preparedness at these licensing hearings was a hoax. Needless to say, the Licensing Board predictably and dutifully licensed the plant.

It was also the TMI-2 proceeding where, for the first time ever in a licensing proceeding, it was shown that the largest source of radioactive emissions in the entire nuclear fuel cycle had been doggedly and resolutely ignored by the NRC. This source of emissions was, of course, the abandoned mill tailings piles. It was my testimony on July 5, 1977, that caused the NRC to act on a long forgotten rule-making petition filed in late 1975 by the New England Coalition on Nuclear Pollution on February 28, 1978. On that day the Commissioners voted to void the 74.5 curie number for radon-222 emissions in the infamous Table S-3 for the special case of TMI-2. On April 14, 1978, this number was struck for all licensed facilities. Yet even with this radon-222 issue unresolved by the Licensing Board, the plant was licensed to operate.

In spite of the seeming irrelevance of the preceding discussion about the TMI-2 licensing process, there is at least one lesson to be learned from this exercise, and that is, there is no problem that any intervenor can raise which will prevent the licensing of any nuclear facility.

The relevance to today's subject is clear. Had I gone before the Licensing Board to address an accident sequence at TMI-2 that included a simultaneous tripping of both feedwater pumps, a pressurizer relief valve that would not close when ordered to do so, both emergency feedwater valves being closed, and so on, it is my considered opinion that I would have been laughed and scolded out of the hearing room. Such an accident, I would have

been told, when the snickering finally subsided, would be hypothetical, speculative, and beyond the scope of the hearing. I must confess, the logic of the Board would have been hard to refute.

Then it all happened, and it happened at TMI-2, in my backyard. All of a sudden, the probability of a serious accident went from being said to be infinitesimally small to unity. And to make matters worse yet, the weather conditions for the first few days after that accident were among the worst imaginable. Situated over the Eastern U.S. was a stagnant air mass. As a result, most of the radioactive materials released in those early days did not dissipate and blow off toward the Atlantic Ocean, instead, they sloshed around like water in a bathtub. This is just one item that the NRC has missed in its cumulative dose estimates. It is not the only one. I am convinced that the 3550 person-rem exposure reported by the NRC between March 28, 1979, and April 7, 1979, is a face-saving, even imaginary value, since it is not supported or supportable by the NRC's own monitoring data.

But in getting back to the subject of reactor safety, I would like to point out that my background is in experimental science. From my own attempts at theoretical calculations, using computer models, and from many years of general observations of theoretical predictions, I have acquired a fairly deep seated mistrust of computer calculations which are not firmly rooted in experimental terra firma.

It is, of course, only through experimentation that we pass judgement on theoretical predictions, conjectures, projections, speculations, and so on. Even some of Einstein's theories have been checked experimentally, and this is as it should be. Yet even in areas where there is an enormous data base for predicting future events, failures of computational predictive techniques still occur. As an example, the U.S. has over 20 years experience at tracking satellites and observing orbital alterations and variations. Even with this backlog of observation and experience, we are still faced with the seeming

certainty that Skylab will reenter that atmosphere, and we will have, at best, just 20 minutes warning. That's not much of a warning. But, we are assured, there is still nothing to worry about, because the overwhelming odds are that it will fall in someone else's backyard.

It does not take much time to discover that in the strange world of a nuclear power industry that was created by Congress and has been both promoted and regulated by one agency, explorations into the basics of reactor engineering, physics, and chemistry have taken a course other than knowledge through experimentation.

If there were a rational regulatory and licensing scheme, the burden of proof in the area of reactor safety would be placed firmly upon the shoulders of the nuclear industry. But the passage of the Price-Anderson Act in 1957 absolved the then infant nuclear industry of its responsibility to the public before the damage was done. This Act established the principle ^{of} that the promotion into existence of an industry where corporate survival was given preeminence above any rights of the members of the potentially affected public. One result of this principle was that it became clear to the infant industry that reactor safety was someone else's responsibility. With the nipple of Price-Anderson firmly in its teeth, a grip which time has only tightened, the nuclear industry assured all who would listen that nuclear reactors were safe enough that even utility executives themselves would have no fear living next to one.

The Atomic Energy Commission (AEC) did not fail to protect and encourage its creation at every step of the way. The Licensing Boards, long before the affected public became aware of what was being perpetrated, developed a genuinely Pavlovian response to any construction permit or operating license submitted.

These Boards' success rates greatly exceed the successful graduation rate from the Oak Ridge reactor operators school.

The contemporary approach is one of safety by edict, procrastination, speculation, economics, double-talk, and ignorance with just an occasional digression into an enormous and largely unplowed field of fundamental reactor research. This is a rather sweeping statement, but it is one that is well supported in history.

As an example, the Loss of Fluid Test facility (LOFT) serves as an excellent case study. This facility was designed to verify the computer programs, or codes, which had been developed to predict the rate of core flooding in a Loss of Coolant Accident (LOCA). Attachment 1 is a copy of two pages from the 1965 report to Congress by the AEC entitled "Major Activities in the Atomic Energy Programs." I repeat, this is from a 1965 report, and from page 186 and 187 of this report it is seen that these very important tests were to have begun in the spring of 1969. Procrastination set in, the completion date slipped, but reactor licensing went on, unhindered by the knowledge that safety systems, upon which tens or hundreds of thousands of lives might depend, had never been tested under realistic operating conditions. Ignorance prevailed and the design effectiveness and functional capability of the ECCS were accepted on the basis of computer calculations, calculated information, and computer speculations, not on the basis of experimental knowledge.

More details on the LOFT facility are presented in Attachment 2, which is pages 851 through 864 of the AEC Authorizing Legislation, Fiscal Year 1972, before the Joint Committee on Atomic Energy, March 4, 1971, Part 2. I call your attention to page 854 where the foremost objective of this program is shown to be experiments to test "analytical methods" pertaining to a LOCA.

Unfortunately, as is seen on page 855, the completion date had slipped from the spring of 1969 to late 1973. Needless to say, the licensing and operation of reactors proceeded.

In Washington, D.C., the Emergency Core Cooling System (ECCS) hearings came and went, and countless flaws in the system were highlighted. But down came the edict that, based on computer calculations, or those "analytical methods" that the LOFT facility was supposed to have verified, everything was alright. Licensing proceeded, unabated.

In the fall of 1978, almost ten years late, the initial experiments at LOFT were conducted, with an electrically heated core. With great fanfare, the NRC announced the success of the test.

Mr. Chairman, when I saw the results of that test a few weeks ago I was stunned. The test had failed. Phenomena were observed in the experiment which were completely unpredicted by the computer code being tested. The results were distributed to numerous Licensing Boards and the parties to each proceeding. Attachment 3 is the notice that was circulated, only after TMI-2. I must emphasize just what the purpose of the test was, and that was to experimentally check the predictive ability of the computer program. A quick reading of this brief notice vividly demonstrated that this goal was not realized; the computer code, called RELAP-4, failed to predict the course the experiment took. And that failure is cloaked in double-talk.

The double-talk comes from the lame explanation put forth by the NRC officials to coverup this obvious failure. That explanation is to characterize the experiment as "atypical." Here the meaning is crystal clear: the computer speculation is being accepted as more valid than experimental results. And licensing goes on.

Over fourteen years of procrastination, edict, speculation and ignorance are now topped with double-talk. Are these characteristics of a research program or a regulatory program that the public should trust or have confidence in? I suggest the answer is no.

It would have been much more difficult for me to appear here today if the LOFT-ECCS fiasco were unique in the nuclear reactor safety research program. However, it is not unique, though the subject of the ECCS has been widely publicized. The fact is, much of the basic research still remains to be carried out. Attachment 4 speaks to this issue. This attachment contains the conclusions from a report released by Oak Ridge National Labs in 1968 entitled "Emergency Core-Cooling Systems for Light-Water-Cooled Power Reactors," by C.G. Lawson. I have taken the liberty to underline a phrase or two, the many conditional verbs, and a couple of sentences. While it is not clear how many of the problems mentioned in this conclusion have been resolved experimentally, I have little reason to believe many have.

Part of the justification for this belief comes from Attachment 2, mentioned earlier. Here I turn your attention to the general testimony of Mr. Milton Shaw, former Director of the Division of Reactor Development and Technology, of the AEC. Mr. Shaw speaks of budget cuts, slowed and curtailed experimental programs, and even questionable information coming out of existing experiments. At one point he states on page 860.

There is also a tremendous controversy as to how beneficial such small-scale experiments can be, but our position is that we can't afford to build them much bigger.

So here is one place where economics plays a key role. Here it should also be noted that in these Hearings, a list of general unsolved problems and areas for research pertaining to reactors was presented on page 852.

These were listed before we became aware, as we have in more recent years, of fuel densification, steam generator tube denting, stress-corrosion cracking and the torus jump problem in BWRs, and so on. And to this short list we must list those generic unresolved safety problems that the NRC annually sends to Congress. No, I don't think we have made much progress in the last 20 years. But this lack of progress has never slowed the relentless licensing of new and larger nuclear power plants.

Let's go back to that recent LOFT experiment. LOFT is a 50 Megawatt Thermal (Mwt) test reactor. Many operating PWRs have thermal outputs between about 2800 Mwt, like TMI-2, to over 3400 Mwt, like Trojan 1. It is evident that the computer code whose accuracy to predict events was being tested, RELAP-4, did not succeed in predicting the course of events. There is an all important question that remains unanswered, and certainly seems to be avoided in silent desperation by the NRC. That question is: what does that experiment at the LOFT facility tell us that is applicable to operating PWRs? Or, do the results of the LOFT facility experiment instill any confidence in RELAP-4 to predict the ability of the ECCS in a large reactor ^{to} carry out its intended function in the event of a LOCA? I can come to no other answer than another negative one.

In northern Pennsylvania, near Berwick, a pair of BWR reactors, Susquehanna 1 and 2, are soon coming up for operating license hearings. The ECNP is an Intervenor in that proceeding and already troubling aspects are arising.

For example, on the subject of power excursions, it appears that great reliance is placed on a computer program dating back to 1956, which, when subjected to preliminary verification experiments, failed in an unsafe direction. (See, for a fuller discussion, "The Accident Hazards of Nuclear Plants," by Dr. Richard E. Webb, University of Mass. Press, 1976, Chapters 3 and 4).

Now, over twenty years have gone by and the question of the susceptibility of large reactors to destructive power excursion accidents does not appear to be resolved, except through speculation, rhetoric, and Licensing Board approvals.

Just last week, we received a communication from the NRC stating that some reports from one of the Susquehanna 1 and 2 subcontractors, Kraftwerk Union Aktiengesellschaft (KWU) are granted an exemption from public disclosure by the NRC. The letter, dated May 11, 1979, is sufficiently vague that it is impossible to determine even the general subject of the now "confidential" KWU reports. The letter contains the following statement

We have also found at this time that the right of the public to be fully apprised as to the basis for and effects of the proposed action does not outweigh the demonstrated concern for protection of your competitive position.

It is certainly not encouraging to learn that the "competitive position" of a subcontractor is more important to the NRC than the right of those affected by some nebulous design feature to know to what kind of risk they are being subjected.

If anything, the TMI-2 accident showed that gaping holes exist in not only our understanding of reactor accidents, but also the ability of not only the NRC to review, inspect, and license reactors, but also of utilities to safely operate them when deviations from anticipated behaviour occur. From the materials I have seen concerning the course and results of this accident, I am exceedingly disappointed in the extremely shallow and unsophisticated nature of the analyses. For example, in a report entitled "Core Damage Assessment for TMI-2," memo from R.O. Meyer to Roger Mattson, April 13, 1979, the heat-up rate of the uncovered core of TMI-2 is discussed, along with the quantity of zirconium fuel cladding estimated to have been consumed by reaction with steam. However, the contribution of heat from the zirconium-steam reaction was neglected in assuming the core heat-up rate. The deficiency here

is because this chemical energy may have been of comparable magnitude to that of the fission product decay heat over the hour or so that the heatup is assumed to have occurred.

Equally unsettling is the rush made by the NRC to apply a series of band-aids to the other operating Babcock and Wilcox (B&W) reactors to get them back to operation as soon as possible. This crash course seems to have preceded an appreciation or even understanding of what the real course of the TMI-2 accident was. To be more precise, it does not appear to be known precisely when the zirconium-steam reaction occurred, or the effect of the electromagnetic relief valve which stuck open in the early stage of the accident. It has obviously been assumed that had this valve properly closed, damage would have been less severe to the reactor. The validity of this assumption has not been established, in my opinion. During most of the initial few minutes of the accident, after the steam generators had boiled dry (at about 1 min. 45 sec. into the accident), water steam flashing through this valve was the major heat release mechanism for the hot core. Had this valve closed properly and stayed closed, the primary coolant system may well have become greatly overpressurized. The rush action by the NRC seems to suggest that the avoidance of the exact sequence of events at TMI-2 is desirable, but it does not appear grounded in a firm understanding of whether or not the recommended solutions might cause worse conditions, should this sequence ever repeat itself.

There is another equally troubling aspect to this whole accident, and that is that TMI-2 was a new reactor with a core that had less than 90 full power days in its operational history. From this fact, it seems necessary to ask whether or not, had this accident happened at a B&W reactor with a higher fission product inventory, like TMI-1, or Rancho Seco, would the results have

been the same? Another seemingly unanswered question is whether or not the quick fix solutions required by the NRC for older operating B&W reactors will work where fission product inventories are higher. It should be pointed out here that higher fission product inventories mean, in general, a higher core heat-uprate. Furthermore, it should be pointed out that the ECCS is designed to function for a relatively cool core, that is, one right after blowdown. It is entirely possible that the actuation of the ECCS onto a hot core, one where the fuel cladding is very hot or melting, may do more harm than good.

The promoters of nuclear power, from the NRC on down, have repeatedly pointed to the supposed "accident-free" or "mortality-free" past history of the commercial nuclear power program. These comments however appealing they might sound, are deserving of a closer scrutiny.

As far as the accident-free part goes, it suffices to say that at least three (3) of the 80 or so nuclear power plants licensed by the AEC/NRC have had very serious accidents early in their respective lives. These were Enrico Fermi I, Browns Ferry 2, and, now, TMI-2. Fermi was down four years for repair. Browns Ferry 1&2 suffered a fire in electrical cables and, for Unit 2, many safety systems were disabled. The third was TMI-2, where half-a million people faced a core meltdown for 4 or 5 days. This is a less than enviable safety record, and it does not include the many other near-misses.

While the validity of the population dose estimates released by the NRC and HEW are not the subject of these hearings, they deserve a few short comments made from my reviewing of the data in report of the Ad Hoc Population Dose Assessment Group. My conclusion is that the members of this group chose to seriously understate the population dose due to the TMI-2 accident. This dubious result was achieved by ignoring completely the character of the data

they had to work with. For most directions around TMI-2, between March 31 and April 7, 1979, the exposures measured by the NRC do not decrease rapidly with increasing distance from the reactor. Quite the contrary, most doses were approximately constant, and some even increased with increasing distance. Unfortunately, the NRC chose not to monitor beyond about 14 miles from the plant, or in the directions in which most of the population was located.

However, the Ad Hoc group used these deficiencies to their own seeming advantage, ignored the trends of the monitoring data they did have, and assumed a standard atmospheric dispersion model to calculate exposures beyond 10 miles from the plant. This model requires that doses decrease according to a minus 1.5 power law, contrary to the existing data out to distances of about 14 miles. As a result, the public exposure widely reported by the press are nothing more than fabrications designed to conceal both the real magnitude of the exposure dose ^{from} to the accident, but also the incredible incompetence of the NRC in its monitoring efforts.

Many people will die as a direct result of the TMI-2 accident. I cannot quantify the number exactly, but I have reason to believe it will number in the hundreds, maybe in the thousands. Efforts by the NRC to conceal this carnage will not solve the problem. Honesty and candor would help, but there appears to be little chance for either in assessing pronouncements from this organization. So licensing must go on, on until we apparently must learn the accident probabilities at nuclear power plants by trial and error. Just what the ultimate toll in human life and misery will be is not predictable, but if Fermi, Brown's Ferry, and TMI-2 are any indication, that toll will be high, both in lives lost and in misery. Tragically, the TMI-2 accident is not over, nor are the releases of radioactive materials.

When all is said and done, the safety philosophy of the nuclear power program, when stripped of the endless self-serving words of praise, and reduced

to how it really works in practice, has been accurately characterized as the Law of the Universe according to Walt Disney, which is

Wishing will make it so

To this fundamental NRC and industry philosophy, I have added two corollaries

1. Wishing that problems were solved is as good as solving them; and
2. Programs can only succeed; failures are simply relabeled as successes.

Evidence of the validity of the first corollary comes from the fact that so many unresolved safety problems remain unresolved after so many years, and so much basic safety research has been postponed and terminated. In addition, the radioactive waste problem and the still nagging problem of low-level radiation persist, even though they have been solved many times through agency and industry press releases.

Failures always become successes in the strange world of nuclear power. The Enrico Fermi accident was one such success. It cost between 60 and 300 million dollars to build, depending on whose figures you believe. It operated for the equivalent of a full month or so before it was mercifully mothballed (but not decommissioned, dismantled, and removed). A lot was learned at the Fermi reactor.

The Browns Ferry fire was also a success because a lot was learned there, like how a core meltdown was averted. Yet today, most reactors are just as vulnerable to fires as Browns Ferry was. So while the \$150 million or so that fire cost taught someone a lot, the lessons yet remain to be applied to many other reactors, but it was a success.

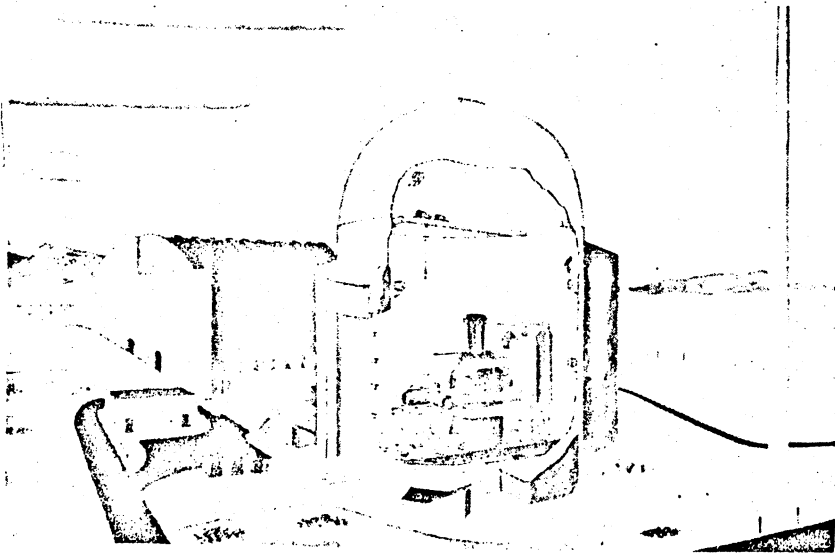
So, of course, was TMI-2 a roaring success. It may be out of service for from 2 or 3 years to forever, it may cost \$300 million to clean it up, or it may be a total loss of over \$700 million. But it was a success. The safety systems worked, and according to the fudged data no one was killed.

These accidents are all part of a strange definition of success, but then, "wishing will make it so."

Gentlemen, who among you would volunteer the constituents of your District or your backyard for the next nuclear "success" story?

Attachment 1

Terrestrial systems. Detailed design of the Loss of Fluid Test (LOFT) facility was essentially completed in December by Kaiser Engineers, Oakland, Calif. A contract to fabricate the containment vessel for the LOFT facility, which will be located at NRTS, was awarded in January to Pittsburgh-Des Moines Co., Pittsburgh, Pa., by M. W. Kellogg, prime contractor for the construction of the LOFT facility. The reactor vessel fabrication contract was awarded in October to the P. F. Avery Corp., Billerica, Mass. Construction of the facility, expected to be complete in late 1967, had passed the 10 percent completion mark by December. Within this reusable test facility, the flatcar-mounted LOFT reactor system will be used to conduct a loss-of-coolant test on a 50-thermal megawatt pressurized water reactor. Following an extensive nonnuclear test program, the



LOFT Facility. Construction reached ground level during 1965 on the Loss of Fluid Test (LOFT) Facility, depicted here by an artist's conceptual drawing. Below-ground-level construction started in October 1964, and LOFT is expected to be operational in late 1967. A cutaway section of the containment shell shows the reactor safety experiment mounted on a double-width flatcar or dolly which can be pulled by shielded locomotive over quadruple rails to a nearby "hot shop" for post-test analysis. One of the principal reasons for building LOFT is to demonstrate the safety of water-cooled power reactors by deliberately triggering a runaway power burst caused by major coolant pipe rupture, a highly improbable but the worst conceivable accident for such reactors. LOFT is part of the safety test engineering program conducted for the AEC by Phillips Petroleum Co.

first nuclear test will be conducted in the spring of 1969. Supporting research and development programs were established at national laboratories and AEC field installations to test equipment and special instrumentation, and to perform analytical studies for predicting the sequence and magnitude of events expected to occur in the LOFT tests.

Aerospace systems. Transient experiments on uranium-zirconium hydride reactors for space nuclear power applications continued during the year at the National Reactor Testing Station. These experiments, conducted by the Phillips Petroleum Co. with the support of Atomics International and Edgerton, Germeshausen, and Grier, Inc., are investigating the kinetic behavior of SNAP reactors when subjected to large and rapid reactivity insertions. The SNAPTRAN-1 series of experiments to investigate the behavior of a reactor in the nondestructive region was completed in September 1965. SNAPTRAN-2, to follow, will project the investigations into the destructive range.

A series of full-scale re-entry flight tests, supported by applied research, have been pursued to determine the effectiveness of using the heat generated by the atmosphere during re-entry to burn up nuclear systems. This burnup, with the subsequent wide dispersal of the debris in the atmosphere, would thus serve as a safe means for radioactive fuel disposal.

During 1965, further analysis was made of the data acquired from re-entry flight tests conducted on a simulated SNAP-10A reactor in May 1963 and October 1964. This flight analysis has provided proof that the specific systems tested would disassemble as designed, and has substantially increased confidence in the ability to predict re-entry heating effects from theoretical analysis.

Effluent Control Research and Development

The programs in effluent control research and development are directed toward the safe management and disposal of various types of radioactive wastes resulting from nuclear reactor operations, the quantitative determination of the behavior of these residual radioactive effluents in the environment, and the development of engineering criteria associated with the environmental aspects of nuclear technology operations. This work provides a basis for defining and controlling the ultimate fate and possible effects of radioactivity in the environment.

Attachment 2

**AEC AUTHORIZING LEGISLATION
FISCAL YEAR 1972**

HEARINGS

BEFORE THE

JOINT COMMITTEE ON ATOMIC ENERGY

CONGRESS OF THE UNITED STATES

NINETY-SECOND CONGRESS

FIRST SESSION

ON

CIVILIAN NUCLEAR POWER PROGRAM

MARCH 4, 1971

PART 2

Printed for the use of the Joint Committee on Atomic Energy



U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON : 1971

sections that we may be obtaining from the machines—are more related to a narrow spectrum of interest, because we just don't have the money to do the broader areas.

In a very real sense, we have had about a 40-percent reduction in this program when one looks at cost of living here since 1969. Certainly the number of people funded by the program has been reduced by about 40 percent in this period some 1,300 people, including many good scientific people, that we just are unable to fund. The number of contractors will have been cut from 54 to 18 by the end of fiscal year 1972. We have had to phase out a number of programs that I predict will affect adversely our long-term outlook and capability in the nuclear power business. Perhaps, if we were doing the work it would prevent us from getting into a lot of trouble, compared to having to bale ourselves out later by leaning back on the people and the technology as a result of present confinements of this program.

I don't know what the solution is, but it is characteristic of the general problem we face.

Representative HOSMER. You mentioned a research and development tax earlier today.

Mr. SHAW. I doubt that the type of tax we talked about will be devoted to this longer term work, which is mostly performed in the laboratories and in the universities, as much as it will be used to build demonstration hardware.

Senator BAKER. I am sort of open on it. We will talk about it some time.

Mr. SHAW. Yes, sir.

NUCLEAR SAFETY

The next area is nuclear safety (fig. 97). Here we are requesting

REACTOR SAFETY PROGRAM PROGRAM ELEMENTS

RESEARCH AND DEVELOPMENT

SUBASSEMBLY TRANSIENT TESTING
FUEL FAILURE PROPAGATION
COOLANT DYNAMICS
FUEL COOLANT INTERACTIONS
FISSION PRODUCT AEROSOLS

ANALYSIS AND EVALUATION

PROGRAM PLANNING
INFORMATION HANDLING
TECH. ASSISTANCE TO REG.
PRESSURE VESSEL STUDIES

RELATED MAJOR FACILITIES

LOFT - LOSS OF FLUID TEST
PBF - POWER BURST FACILITY
CDC - CAPSULE DRIVER CORE
WSEP - WASTE SOLIDIFICATION ENGR. PROTO.
TREAT - TRANSIENT REACTOR TEST

* FUNDED UNDER CIVILIAN POWER PROGRAMS.

EFFLUENT CONTROL

ENVIRONMENTAL INVESTIGATIONS
THERMAL EFFECTS STUDIES
WASTE TREATMENT & DISPOSAL

ENGINEERING FIELD TESTS

LOSS OF COOLANT TESTS AND
EMERGENCY CORE COOLING
INVESTIGATIONS

ENGINEERED SAFETY SYSTEMS

CONTAINMENT TECHNOLOGY
PLANT APPLICATIONS & ENG. TEST
PROGRAM
STANDARDS, CODES, SPECIFICATIONS

GEOLOGIC SEISMIC FACTORS

BASIC GEO-SEISMIC DATA
ENVIRONMENTAL MAPPING
LIAISON WITH OTHER GEO-SEISMIC
PROGRAMS

* DEVELOP ASEISMIC DESIGNS & DATA
* SPECIFIC SITE INVESTIGATIONS
* DEMONSTRATION OF ASEISMIC DESIGNS

\$35.9 million for fiscal year 1972, which is the same as the 1971 estimate. The major increase is in fast reactor safety, which has been increased in our projections from \$7.4 million to \$10.6 million. Of course, with the level budget this increase has had to be offset by decreases in several other vital or important safety areas. These decreases include no further fuel procurement in certain of the test reactors, particularly the power burst facility and cutback of other light water safety work.

For example, we have had to terminate programs related to failure modes of zirconium-clad fuel rods which are used in light water reactors. This work was being performed at Oak Ridge. Again we would like to continue that work, which is out-of-pile work, but we feel we must go in-pile with some of this zirconium work to build on the out-of-pile work already accomplished.

The waste solidification experimental program (WSEP) underway at Hanford is being phased down and will be closed out in 1972. Much of the work on pipe ruptures and reactor accident analysis that was going on in a number of organizations will be phased out. Some of these activities are already phased out in order to consolidate work in a small number of organizations.

Of course, we are investigating work on siting and safety problems which are of general applicability not only to the commercial reactors, or potentially commercial reactors, but also for reactors of our own. This includes our test reactors and other facilities, for which we must do safety work in order to assure the continued safe operation of these facilities. Examples of the type of requirements placed on the nuclear safety program are those shown on figure 98, and those that arise from a detailed analysis of the accident sequence diagram, figure 99.

REACTOR SAFETY PROGRAM

ACRS "ASTERISKED" ITEMS

1. THERMAL SHOCK TO PRESSURE VESSEL FROM ECCS OPERATION.
2. SEISMIC INSTRUMENTATION FOR STRONG-MOTION RECORDING.
3. IMPROVED PRESSURE VESSEL FABRICATION AND IN-SERVICE INSPECTION TECHNIQUES.
4. CALCULATIONAL MODELS FOR REACTOR BLOWDOWN.
5. FUEL FAILURE MODE IN LOSS-OF-COOLANT-ACCIDENT AND EFFECT ON ECCS CAPABILITY TO PREVENT CLAD MELTING.
6. FUEL FAILURE-LOSS-OF-COOLANT-ACCIDENT ANALYSIS AT CURRENT HIGH POWER DENSITIES AND BURNUPS.
7. EFFECT OF SUBASSEMBLY FLOW BLOCKAGE.
8. EFFECT OF END-OF-LIFE TRANSIENTS ON FUEL FAILURE.
9. DETECTION OF GROSS FUEL ELEMENT FAILURES.
10. SEPARATION OF CONTROL AND PROTECTION INSTRUMENTATION (DESIGN).
11. HYDROGEN EVOLUTION
12. VITAL EQUIPMENT SURVIVAL IN A LOSS-OF-COOLANT ACCIDENT.

FIGURE 98

ACCIDENT SEQUENCE DIAGRAM WITH ENGINEERED SAFETY FEATURES

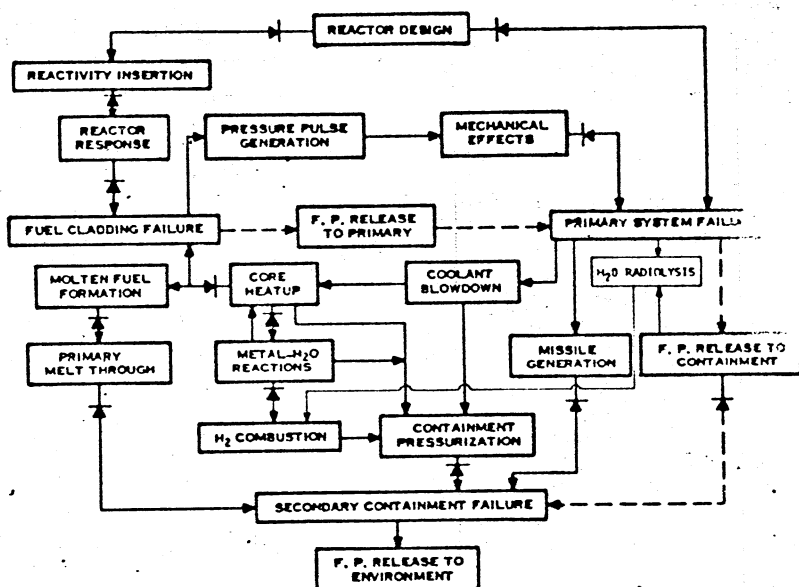


FIGURE 99

LOFT PROGRAM

Principal areas for hardware and fuel commitments in this budget category currently are in the LOFT program, which is the loss of fluid test facility being built at Idaho, as well as in the power by facility program at Idaho. The LOFT budget represents \$9.9 million, which is an increase over fiscal year 1971 of \$1.8 million. This increase is principally due to the fabrication and assembly of large components for this unique facility. It is the only facility in the world in which we will be able to obtain large-scale reactions to a loss of coolant accident and study the related phenomena from actually using emergency core cooling systems in an operating reactor.

Of course, this is one of the principal areas that has been discussed and debated heavily in the safety circuit; that is, this tremendous concern over a loss of coolant. For example, if a pipe ruptures, does loss of coolant occur rather quickly? Is one able to inject water quickly into the reactor? What will be the effect of doing this? This, of course, is one of the principal areas of interest in the licensing of light water reactors. We are quite pleased with the regrouping at Idaho in the LOFT project. The project design is moving ahead quite well now, and we believe that the facility, if funding remains compatible with what we have scheduled, can be brought into use within the next 3 years.

Representative HANSEN. May I ask a question here, Mr. Chairman?

Representative PRICE. Mr. Hansen.

Representative HANSEN. To what extent will LOFT yield some of the answers that may be needed in the area of safety for the fast breeder reactor, gas cooled reactor or other concepts?

Mr. SHAW. Very little, sir. LOFT is principally related to safety evaluations for the pressurized water reactor. It has some value to understanding some of the parts of the boiling water reactor, but is principally directed around the pressurized water reactor safety considerations.

Its contributions to the other reactors will be principally along the lines of being able to relate analytical work to experimental results, and individual separate effects tests as they relate to the whole. That is, it will give the confidence to the analytical people and relate analysis to the experimental results to permit carry-over into other concepts.

That is about the limit of it, sir.

(Testimony continues on p. 858)

(Additional information provided for the record follows.)

LOFT

Significant progress has been made in the design and construction of the 55 MWt Loss of Fluid Test Facility (LOFT). LOFT is the only nuclear facility in the world planned to conduct major loss-of-coolant accident experiments (see chart below for LOFT experimental objectives.)

LOFT

EXPERIMENTAL OBJECTIVES

1. TEST THE ADEQUACY OF ANALYTICAL METHODS USED TO PREDICT:
 - a. THE LOSS-OF-COOLANT PHENOMENA AFFECTING CORE THERMAL RESPONSE;
 - b. THE CAPABILITY OF THE EMERGENCY CORE COOLING SYSTEM (ECCS) TO FULFILL THE INTENDED FUNCTION;
 - c. THE MARGINS OF SAFETY INHERENT IN THE CAPABILITY OF THE ECCS;
 - d. THE THERMAL AND MECHANICAL RESPONSE OF THE CORE AND PRIMARY SYSTEM COMPONENTS;
 - e. THE PRESSURE-TEMPERATURE RESPONSE OF THE CONTAINMENT ATMOSPHERE; AND
 - f. THE MAGNITUDE, COMPOSITION, AND DISTRIBUTION WITH RESPECT TO TIME OF THE FISSION PRODUCTS IN THE CONTAINMENT BUILDING.
2. VERIFY THE DESIGN REQUIREMENTS WHICH DETERMINE THE CAPABILITY OF THE ECCS AND THE PRESSURE REDUCTION SYSTEM TO FULFILL THEIR INTENDED FUNCTION.
3. REVEAL THRESHOLDS OR UNEXPECTED PHENOMENA WHICH AFFECT THE VALIDITY OF THE ANALYTICAL METHODS USED TO PREDICT THE EFFECTS OF A LOSS-OF-COOLANT ACCIDENT AS LISTED ABOVE.

The importance of an actual power reactor plant to conducting these experiments cannot be underestimated. As noted in previous hearings, the overall LOFT effort has been successful in (1) providing a focal point and a fundamental sense of direction to the water reactor safety program, (2) forcing investigators to face the reality of an actual power reactor in the accident mode, and (3) providing a central vehicle to build and hold a competent safety oriented technical staff in a vital national program. The fundamental soundness of the LOFT objectives have been reinforced by continued engineering and analysis of LOFT which has further established the relationship of the LOFT program to the current industry light water reactors. This has also been reconfirmed by reviews conducted by industry consultants, the AEC Regulatory Divisions, and the ACRS.

LOFT DESIGN AND CONSTRUCTION

The project design has progressed to the point that procurement of all the major reactor plant components is underway. System design descriptions of almost all major plant systems have been completed by INC. In addition, 10 water reactor major component standards and associated LOFT specifications have been approved by INC and AEC. As a result of this engineering progress, procurement action is underway on the reactor pressure vessel modifications, steam generator, pressurizer, primary reactor piping, and reactor support frame. Work has been initiated on reactor vessel modifications. The design of the reactor core and vessel internals and associated in-core instrumentation is well underway. This is a large effort since the core will be heavily instrumented in order to derive the experimental information. In addition to those RDT water reactor standards that have been approved there is work underway on 25 standards which are being prepared with the help of ORNL.

Design and construction of LOFT construction funded facilities continues with the status at about 90% of design and 60% of construction completed. During the past year the basic containment structure including the large railroad door and frame have been completed and considerable outside concrete was poured. Design and procurement work is underway on the reactor auxiliary systems with additional concrete pours and final containment tests planned for later this year. In order to efficiently complete the project certain experimental equipment of low priority such as an extensive fission product sampling system has been deferred.

As reported last year, the overall plant continues to be scheduled for late 1973 initial operation. However, difficulties are still being encountered due to the short supply of experienced water reactor design and manufacturing personnel and the problem of obtaining small one-of-a-kind high quality components, instruments and equipment from industrial sources that are heavily committed to the large scale manufacture of equipment for the large commercial water reactors.

EMERGENCY CORE COOLING AND RELATED RESEARCH

As part of the LOFT R & D support effort, various emergency core cooling analytical studies and separate effects tests are in progress as indicated below. The results of these efforts form the basis for planning LOFT experiments and the basis for direct technical assistance to the AEC Division of Reactor Licensing.

Analytical studies and code development at BMI-Columbus will be terminated at the end of FY 1971. Analytical studies, code development and assistance to AEC regulatory divisions will continue on through FY 1972 in support of LOFT.

Blowdown experiments on the scaled reactor system (semiscale system at INC) will continue on through FY 1972 in support of LOFT. The intent of these tests is summarized in the following chart:

REACTOR SAFETY PROGRAM

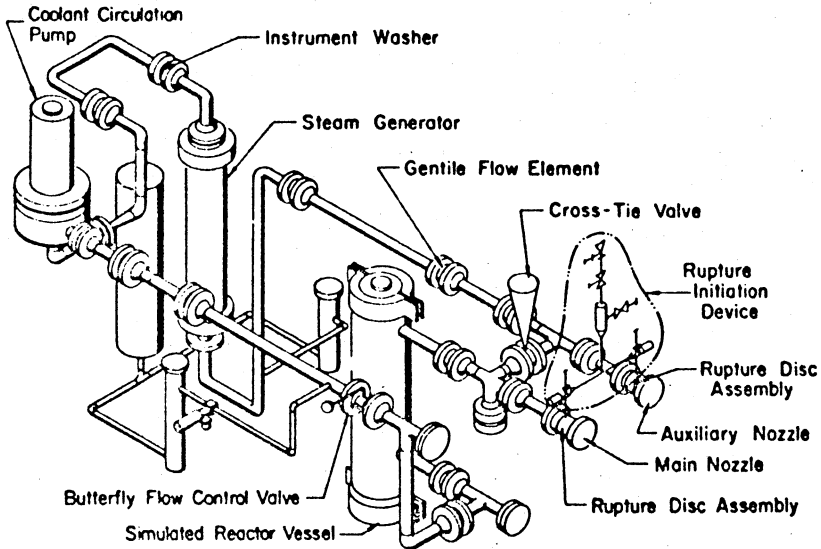
EMERGENCY CORE COOLING SYSTEM (ECCS) TESTS

THE OVERALL INTENT OF THE SEPARATE EFFECTS TESTS IS TO PROVIDE:

1. EARLY SCOPING INFORMATION TO ASSIST IN THE DEVELOPMENT AND EVALUATION OF ANALYTICAL TECHNIQUES OVER A WIDE RANGE OF VARIABLES.
2. INFORMATION ON THE CONTROLLING VARIABLES WHICH ULTIMATELY DETERMINE THE PERFORMANCE REQUIREMENTS OR CRITERIA FOR THE EMERGENCY CORE COOLING SYSTEM.
1. INFORMATION TO ESTABLISH INITIAL TEST CONDITIONS FOR THE LOFT INTEGRAL TEST SERIES AT THE MOST SEVERE DEMAND CONDITIONS FOR THE EMERGENCY CORE COOLING SYSTEM.
1. PARAMETRIC INFORMATION FOR USE IN THE ANALYSIS TO PROVIDE FOR EXTREMES OF FLUID ENVELOPE GEOMETRIES AND BREAK CONDITIONS CHARACTERIZING THE CURRENT AND NEAR FUTURE PRESSURIZED WATER REACTORS.

The semiscale system shown below was modified as reported last year for simulated core heat and again this year for emergency core cooling injection. Future plans call for scaled multiloop system modifications.

SEMISCALE SYSTEM DOUBLE ENDED BREAK CONFIGURATION

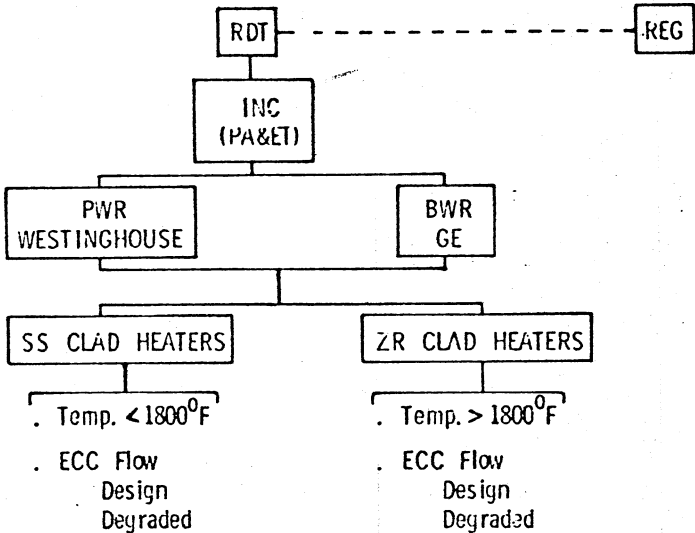


A series of tests have been run in the semiscale apparatus using simulated core heat (electric heaters) and accumulator injection of emergency core cooling (ECC) water. The conditions of the tests are as typical of large PWRs as the scaled model will permit. The results are being used to check analytical models, evaluate ECC systems and provide data for LOFT. The results are also being provided to industry as rapidly as obtained and its support is being solicited. Six tests to date have experienced difficulty in injecting ECC accumulator water into the core region under PWR loss-of-coolant-accident conditions because of apparent bypass of the ECC water. The apparatus will be modified by early FY 1972 to more realistically study this problem using LOFT geometry and system conditions more closely representative of those of commercial reactors.

Testing of emergency cooling capability was completed using full size (12 ft. long) pin assemblies in the Full Length Emergency Cooling Heat Transfer Pro-

gram (FLECHT) at GE and Westinghouse under subcontract to Idaho Nuclear Corporation (INC), as shown below.

REACTOR SAFETY PROGRAM
FULL LENGTH EMERGENCY COOLING HEAT TRANSFER (FLECHT)



These tests, in which electrically heated assemblies simulated decay heat generation in full size reactor fuel pins cooled by sprays and flooding, were needed to assess emergency cooling system performance under design and off-design conditions. The tests performed indicate that under most emergency conditions postulated, the emergency cooling systems will perform their intended function over a wide range of cooling and temperature conditions. However, this confidence level becomes reduced under certain combinations of clad temperature and reduced or delayed flow conditions as might be reasonably postulated for higher operating power densities characteristic of future nuclear plants. Under some of these extreme conditions tested in the FLECHT projects, 49 pin bundles were damaged as the zircaloy passed the time-at-temperature thresholds associated with chemical reactions between clad and water or steam. Information of this type was considered valuable in demonstrating and bracketing areas of concern in the design of future emergency cooling systems. The limitations of these tests, such as lack of complete system simulation and the use of electrical heaters which failed when extreme conditions were imposed, were recognized and taken into account in interpreting the data.

As a result of the FLECHT project, a better understanding is available on the interactions between emergency coolant (assumed capable of delivery to the core within 15-30 seconds from a major coolant pipe break) and the zircaloy cladding (assumed to heat up from a combination of stored fuel energy at the time of the pipe break, plus the loss of coolant plus decay heat generation). However information gaps remain in the time regime following the assumed pipe break, but prior to ECC injection. During this regime, stored fuel pin heat is transferred to the cladding, to the remaining coolant, and to steam formed during system depressurization. The rate and amount of heat transferred during this time period, called the Blowdown Heat Transfer (BDHT) regime, is important in establishing the cladding temperature at the time of emergency core cooling injection. The importance of obtaining BDHT information, for both pressurized and boiling reactors, is recognized by the industry, as well as the AEC Development and Regulatory Divisions.

In recognition of this common need, the Division of Reactor Development and Technology has held discussions with PWR and BWR vendors to encourage cooperative efforts between industry and the AEC to study the BDIT regime with experiments sealed to represent the major components of operating power plants. General Electric has proposed a shared cost cooperative program on BDIT for BWR's, and RDT has agreed in principle, assuming that mutual agreement on work scope and contract conditions can be obtained.

POWER BURST FACILITY (PBF)

Mr. SHAW. The power burst facility is a reactor for testing effects of fuel failures resulting from a burst mode or steady state operation (fig. 100). We put fuel samples that have an operating history—

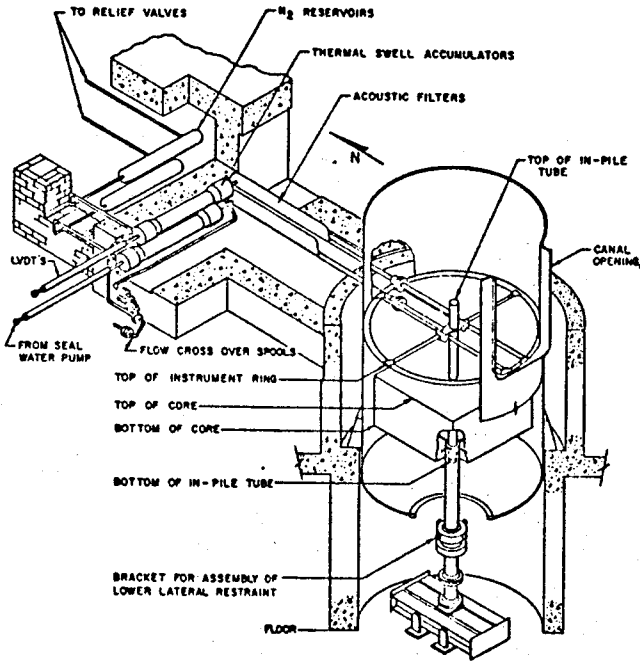


FIGURE 100

that is, have previously been irradiated—and give them a nuclear pulse or give them an overpressure or power to flow imbalance, in order to see the types of failures that we may induce and the consequences of these failures.

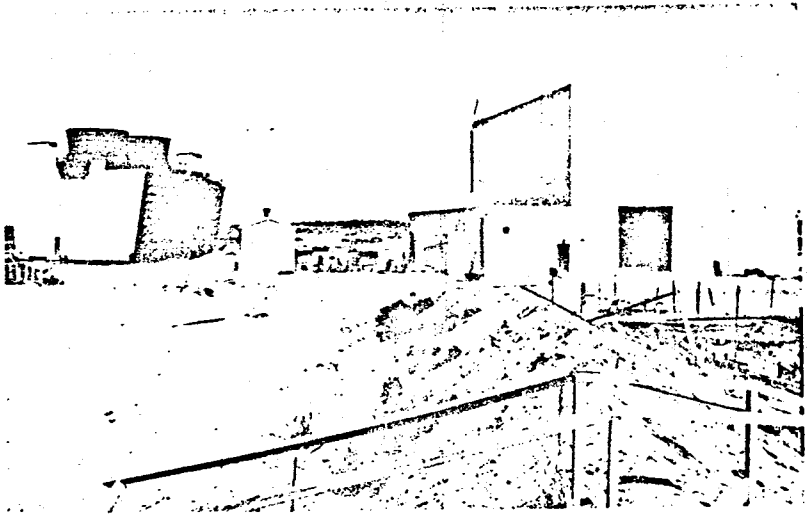
Of course, to do this, we have a special closed loop in the power burst facility, such that when the failure occurs it does not affect the rest of the system.

(Additional information provided for the record follows:)

POWER BURST FACILITY

The Power Burst Facility (PBF), (shown in chart below) being completed at NRTS, is an oxide-fueled, epithermal, water moderated reactor capable of steady-state and transient operation including the performance of power bursts having initial periods approaching 1 msec. Fuel loading is scheduled for CY 1971 and the start of the experimental program is scheduled for early CY 1972. On October 29, 1970, responsibility for the PBF was transferred from the construction

contractor, Howard S. Wright and Associates, to the operating contractor, Idaho Nuclear Corporation. On December 11, 1970, the efforts of the architect-engineer, Ebasco Services Inc., were terminated.



POWER BURST FACILITY. View looking northeast showing cooling tower on left, emergency generator in center, and PBF reactor building on right.

The overall objectives of the Power Burst Facility is to provide a safety test facility for conducting research on accidental melting of reactor fuel samples and assemblies (See chart below) Such information is vitally needed to supplement the out-of-pile work on fuel assembly mock-ups which have been undertaken to study fuel failure modes and emergency cooling effectiveness using electrical heaters (e.g., FLECHT program). By performing fuel assembly tests in PBF it will be possible to more realistically predict full scale reactor core behavior under equivalent accident conditions. Analyses presently conducted on full scale systems are deemed to be conservative in the determination of accident consequences—but significant experimental proof is lacking.

REACTOR SAFETY PROGRAM
POWER BURST FACILITY (PBF)

- OBJECTIVES :
1. TO STUDY NUCLEAR FUEL AND CLADDING BEHAVIOR OF FUEL PIN CLUSTERS UNDER ABNORMAL OPERATING AND POSTULATED ACCIDENT SITUATIONS TO DETERMINE SAFETY MARGINS.
 2. TO IDENTIFY ANY UNEXPECTED EVENTS OR THRESHOLDS NOT PRESENTLY ACCOUNTED FOR IN THE ANALYSIS OF FUEL AND CLADDING RESPONSE.
 3. TO EVALUATE THE ADEQUACY OF ANALYTICAL MODELS TO PREDICT THE CONSEQUENCES OF POSTULATED ACCIDENTS IN NUCLEAR REACTORS.
- DESCRIPTION :
- SAFETY TEST REACTOR, CONTAINING A DRIVER CORE WITH A CENTRAL PRESSURIZED WATER LOOP DESIGNED TO TEST THREE-FOOT LENGTH PWR OR BWR FUEL ASSEMBLIES, CAPABLE OF STEADY-STATE AND TRANSIENT OPERATION.
- EXPERIMENTS :
- LOSS-OF-COOLANT, POWER-COOLING-MISMATCH, AND REACTIVITY-INITIATED TESTS WITH SINGLE PIN AND MULTIROD CLUSTERS USING UNIRRADIATED AND IRRADIATED PWR AND BWR FUEL FOR CONDUCTING RESEARCH ON MELTING OF REACTOR FUEL SAMPLES AND ASSEMBLIES.
- STATUS :
- FACILITY COMPLETION AND FUEL LOADING DURING CY 1971 AND START OF THE EXPERIMENTAL PROGRAM IN EARLY CY 1972.

The basic document which will focus on the experimental program in relation to the current safety issues and priorities is the PBF Program Plan, an outline of which was circulated to the ACRS and the AEC regulatory staff in May 1969 and to industry in November 1969. Based on ACRS, regulatory staff, industry and RDT review and comment, INC is in the process of establishing a firm test program for the initial testing series and outlining the long term testing series. Present program plans are devoted to water cooled reactor fuels and emphasize the simulation of those accident conditions considered most representative of the route by which reactor fuel melt might be achieved. Exploratory work will continue on the possibility of testing other fuel types. Some facility modifications are being considered which, if incorporated, would provide the PBF with increased capability to model the potential accident conditions of advanced high power density reactors.

The Capsule Driver Core (CDC) program, which provided failure data on individual pins under static coolant conditions as a prelude to more complex tests of fuel clusters in the Power Burst Facility, was terminated during FY 1971.

Mr. SHAW. The unfortunate part about every one of these facilities is that they are quite expensive to build and quite expensive to operate. But we know of no other way to get the kind of data we need. There is also a tremendous amount of controversy as to how beneficial such small-scale experiments can be, but our position is that we can't afford to build them much bigger.

These data become very significant in terms of insuring analytical and experimental results. We believe we have to keep this kind of effort going to provide the best possible answers to the concerns that can be expressed by those looking at what happens if many things go wrong and if systems put in to take care of these accidents don't work.

FUNDING OF SAFETY PROGRAM

Representative HANSEN. My concern, if I can express it, is that really we may not be moving ahead fast enough in terms of the funding, of the kind of safety research that will help produce the answers to the growing concerns that are being voiced, particularly by environmental groups; safety being such an important part of reactor technology as the units grow in terms of size, it seems to me that we are going to have to keep pace in the level of effort that we are mounting for reactor safety.

My concern is what appears to be a tapering off in the area of safety research just at the time that we probably ought to be stepping it up.

Mr. SHAW. Mr. Hansen, it is no secret that there are strong feelings and representations that say exactly what you have said. We certainly are not getting what we have asked for in reactor safety funding.

The people concerned must recognize that without the data, there has to be some compensating action taken, such as in terms of being more conservative and more careful than might otherwise be necessary. We cannot exploit the reactors or push the reactors as hard as we believe they could be operated.

We feel we have to develop on two fronts; that is, strong quality assurance programs but still examining to our best possible ability what happens if things go wrong and get the signs of problems early enough and exercise the type of control needed.

It is true that partially as a result of the need to increase the advanced reactors safety programs, we have had to back off on the light water safety programs. We have had a number of meetings with the industrial groups in order to try to get them to pick up these light water safety activities. There is a good agreement that something

like this will have to be done, but we haven't moved ahead as quickly as should have been done.

We feel we have excellent facilities in house. We have excellent people; but we feel that the industry should really be supporting more of these activities before we terminate them completely. We need to get many of the answers that must be available if we are to continue to live with the analyses and assumptions made on such matters as failure modes and response of safety systems with increased power density and certain materials and operating patterns.

I want to note, however, that the worth of the safety program relates not only to the timing of initial start up of these plants, but also throughout the operating history.

Many of the safety concerns you hear about right now relate to the consideration of long-term operation, which we think are very legitimate. We feel that this concern over safety is the kind of thing we must keep in front of us and talk about openly.

The safety program suffers the disadvantage of open discussion although we feel it is the right way to do it. We have discussed safety plans; we have identified all the problems and many of these may not be real. Unfortunately, our critics and intervenors are using much of this information against nuclear power in many cases. We feel we have no option but to conduct the safety related programs this way and accept the criticism and the consequences.

Representative HANSEN. What is the request for safety?

Mr. ABBADESSA. The division request was for \$49 million. The agency request was \$42 million, and the budget that you are looking at, Mr. Hansen, has \$35.9 million, which is the prior year's level.

(Testimony continues on p. 864.)

(Additional information provided for the record follows:)

NUCLEAR SAFETY PROGRAM

The Nuclear Safety Program is divided into five budget categories—Nuclear Safety Research and Development, Effluent Control Research and Development, Engineering Field Tests, Reactor Safety Analysis and Evaluation, and Engineering Safety Features.

The FY 1972 funding request for Nuclear Safety Research and Development is \$14.4 million, an increase of \$1.4 million above the current FY 1971 estimate. This represents an increase of \$3.2 million for LMFBR safety R&D, part of which is offset by reductions in AEC funding for the Power Burst Facility program and by completion of a study of failure modes in light water reactor fuel cladding. The increased LMFBR safety R&D funding is for expanding programs in the areas of fuel element failure propagation, fuel-coolant interactions and post-accident heat removal, and for test irradiations.

The FY 1972 funding request for Effluent Control Research and Development is \$4.0 million, a decrease of \$1.5 million below the current FY 1971 estimate. This activity is directed toward developing safe, practical methods for long term management of the radioactive wastes resulting from nuclear facility operations; determining and assessing the fate and behavior of these residual radioactive wastes in the environment, and with the geophysical and environmental aspects of siting, design and construction of reactors and related nuclear facilities. The decrease in requested funding is made possible by the achievement of viable, tested methods of waste solidification and permanent storage in salt mines, by a reduced need for additional work in radioactive residue process development, and by the completion of meteorological studies at the National Reactor Testing Station. Increases accommodated within this budget element provide for the conceptual design and environmental evaluation of the National Radioactive Waste Repository planned to be constructed at Lyons, Kansas.

The fiscal year 1972 funding request for Engineering Field Tests (LOFT) is \$9.9 million, an increase of \$1.8 million over the current fiscal year 1971 estimate. LOFT fuel fabrication will be initiated in fiscal year 1972. LOFT analytical systems

design has been reduced but increases are necessary in test assembly fabrication fuel fabrication and operations planning.

The fiscal year 1972 funding request for Reactor Safety Analysis and Evaluation is \$1.1 million, a decrease of \$0.1 million below the current fiscal year 1971 estimate. A small computer activity for the handling of data on safety-related reactor characteristics is being terminated, as is the High Temperature Gas Reactor Program Office. A small increase in funding is requested for the Nuclear Safety Information Center.

The fiscal year 1972 request for Engineering Safety Features is \$6.5 million, a decrease of \$1.8 million below the current fiscal year 1971 estimate. This activity provides a program for investigation and development of effective engineered safety features to prevent major accidents and to control their consequences in the unlikely event they should occur. Under this budget category, efforts in "separate effects" testing to study experimentally the individual phenomena contributing to reactor behavior under accident conditions have been considerably reduced from fiscal year 1971 levels. Analytical study of loss-of-coolant accidents and the standards program have also been reduced. The Containment Systems experiment (CSE) has been terminated. Significant increases over fiscal year 1971 levels are planned in the study of reactor system and containment structural dynamic response to accident conditions and in LOFT integral experiment work and radiological studies. Work is being completed and closed out in experiments on initiation of ductile pipe rupture, in evaluation of existing data to describe reactor accidents, and in spray and pool absorption technology. A new program to study blowdown heat transfer, cooperatively funded with industry, is being initiated in fiscal year 1971 and will be continued in fiscal year 1972.

While the Nuclear Safety Program budget is organized on the basis of the five categories previously described, the description included in the record of this hearing of the program is provided with reference to particular applications, and emphasis is placed on specific accomplishments during the past year. The breakdown of the nuclear safety budget for FY 1972 according to these applications is as follows:

	<i>Dollars in millions</i>
Fast breeder reactor safety	11.1
Light water reactor safety	16.4
Environmental effects	4.0
High temperature gas reactor safety	0.5
Standards and codes	2.6
Other	1.3
Total	35.9

(Subsequent to these hearings, the committee submitted the following questions to the Commission for reply:)

Question: What type of additional work would be conducted in the safety program if the funding level were at the division request instead of the requested \$35.9 million?

Reply: The nuclear safety program, to stay within the ceiling of \$35.9 million has undergone serious project reductions. Since certain projects require increased support, others must be reduced. If increased funding were available, efforts would be supplemented in both fast and thermal reactor safety. Additional fast reactor safety effort would be undertaken as follows:

1. Acceleration of TREAT modifications to improve testing capability; e.g., converter region.
2. Alternate shutdown system studies and experiments for LMFBR's.
3. Study of plant size effects on LMFBR potential safety issues.
4. Accelerated effort on post accident heat removal studies and experiments.

Thermal Reactor Safety programs would be complemented as follows:

1. Implementation of additional Blowdown Heat Transfer, engineering scale experiments for loss of coolant accident studies applicable to PWR systems.
2. Increase of effort and acceleration of Blowdown Heat Transfer, engineering scale experiments for loss of coolant accident studies applicable to BWR systems.
3. Development of integrated multidimensional computer codes for analysis of loss of coolant accidents.
4. Acceleration of the PBF program for early initiation of power coolant mismatch and loss of coolant experiments of irradiated fuel assemblies.

5. Acceleration of PWR Scaiscale testing of loss of coolant behavior and emergency core coolant injection systems including experiment modifications to resolve potential deficiencies in ECC coolant delivery.

6. Initiation of containment studies applicable to BWR pressure suppression systems.

7. Experimental investigation of fuel failure modes under simulated reactor coolant blowdown conditions.

8. Performance of low flooding rate, atmospheric pressure tests in FLECHT PWR geometry.

9. Increase the level of effort related to primary system integrity, specifically, implementation of tasks on stress corrosion, pipe rupture studies, Heavy Section Steel Technology program and stress indices for piping, pumps and valves.

Question: Would you please provide a narrative explanation of the steadily increasing operating costs indicated in your 5-year projections from FY 1972 through FY 1977 for the nuclear safety program?

Reply: These projections have the following basis:

1. Water reactors built in the future will incorporate essentially present day major design and engineering features.

2. Although base technology requirements are decreasing, requirements for engineering safety systems offset this to provide a near-term overall funding peak for water reactor safety. The water system safety program will then phase down to a base level to keep pace with evolving new technology.

3. The orderly reduction of water reactor safety efforts will be paralleled by an increasing emphasis of support on advanced reactors.

4. There will be a continuing emphasis on support activities, including work related to small radioactive spill problems, efforts on standards and environmental R&D in such areas as radioactive waste management and thermal effects.

Part of the near-term water reactor safety funding peak can be attributed to the current effort required to resolve uncertainties facing both reactor suppliers and those charged with safety assessment for the surge of commercial reactor business which occurred between 1965 and 1968. It can be predicted that the majority of the reactor safety questions will be answered for this reactor type by the time most of these reactors have been granted operating licenses, which is projected to occur by 1975, if funding and other resources are made available.

In the near term, LOFT and PBF require extensive support from the operating budget in the form of research and development to provide a basis for their design, construction and operation, and to pay for expendable items such as reactor cores and experimental components. Continued funding will be necessary also for the development of safety technology associated with larger-sized water reactors, new applications, higher power densities, reduced design margins, and siting closer to high concentrations of population. It will also be necessary to continue to provide a technological safety basis for the design, construction, operation and maintenance of advanced light water reactor plants, and for their safety assessment for regulatory purposes.

Funding requirements for breeder reactor safety R&D are expected to increase significantly over the period of the next decade. Consistent with the establishment of the LMFBR as the highest priority program for achieving the breeder objective, most of the projected funding is directly related to this advanced concept. It should be noted, however, that the safety program will also benefit other advanced reactor concepts. For example, some of the test facilities to be built for the LMFBR program could be used for R&D on other advanced reactor concepts.

These projections in general are based on the widespread use of the uranium-plutonium fuel cycle, and could be significantly altered if in the future it becomes necessary from the standpoint of national interest to undertake an increased program for use of the thorium-uranium fuel cycle.

The funding projection also provides for the continuation of modest R&D support on the effects of nuclear power on the environment. This work is even more essential now in light of the national concern regarding the environment. Additional R&D on waste management techniques will be required. It is also planned to increase efforts, in concert with other Federal agencies and industry, on the control of the discharge of heated effluents from nuclear power plants and the effect of these discharges on the environment. This planned increase is consistent with the recommendation by the JCAE for an increased effort to provide information to answer the questions related to environmental effects of nuclear power plants.

Question: Could you also discuss the reasons for the projected construction cost increases in the nuclear safety program for FY 1973 through FY 1977?

Reply: The primary reason for the increase relates to the safety test facility and loops as shown below:

Safety test facility and loops:	Millions
Fiscal year 1973.....	\$12
Fiscal year 1974.....	55
Fiscal year 1975.....	20

This projection provides for design and construction of new facilities for the conduct of LMFBR safety experiments, should studies presently underway indicate the need for such facilities. The most important types of tests will be those in which the experiment (one or more LMFBR-type fuel subassemblies) is first brought to full power, steady-state conditions and then exposed to an overpower, transient, flow coastdown, flow blockage, or a comparatively slow change in reactivity. Fast insertions, either from low power or full power conditions, also are to be considered and will place different demands on the facilities.

Mr. JOHNSON. Mr. Hansen, there is some philosophy within various quarters that as reactors get developed and become established and useful, industry should pick up more of the tab for keeping on to the safety program. It is a difficult thing to do actually because, as Mr. Shaw said, it is not quite the same as testing an airplane. The cost of the airplane is handled by the manufacturing company and FAA just goes out and checks it and tests it.

In this case, we have to build special facilities. I think we are doing about the best we can to get as much money as we can to keep the program going. It is difficult to get more support than that.

Dr. KAVANAGH. We have been trying very hard to get more funds for this program. I think what you have said in your question is correct. There should be more in it. We are working to get better cooperation in reactor safety programs.

This does not mean that our reactors are not safe. It means that we should be spending more to assure that they are safe, to gain added assurance that they are safe and, as Mr. Shaw says, find it possible to extend the operating limits and still maintain safety.

(Additional material from Mr. Shaw's prepared statement follows:)

FAST REACTOR SAFETY

The main areas of investigation in the fast reactor safety program are following the priorities established in the national LMFBR program plan, basically developed by detailed analysis of the LMFBR accident sequence diagram, figure 101.

Attachment 3

UNITED STATES
 NUCLEAR REGULATORY COMMISSION
 WASHINGTON, D. C. 20555

April 5, 1979

BOARD NOTIFICATION

Re: Cherokee 1-3	Docket No. 50-491-2-3
Diablo Canyon 1-2	Docket No. 50-275-323
FNP	Docket No. 50-437
Greene County	Docket No. 50-549
Jamesport 1-2	Docket No. 50-516-7
Marble Hill 1-2	Docket No. 50-546-7
McGuire 1-2	Docket No. 50-369-70
North Anna 1	Docket No. 50-338-9
Pebble Springs 1-2	Docket No. 50-514-5
Perkins 1-3	Docket No. 50-488-89-90
Pilgrim 2	Docket No. 50-471
Seabrook	Docket No. 50-443-4
Shearon Harris 1-4	Docket No. 50-400-1-2-3
Sterling	Docket No. 50-485
St. Lucie 2	Docket No. 50-389
Three Mile Island 2	Docket No. 50-320
Tyrone	Docket No. 50-484
Wolf Creek	Docket No. 50-482
WPPSS 4	Docket No. 50-513

Distribution:

Copies of a "Board Notification" dated April 5, 1979, have been served on the following persons. Those whose addresses are at the U.S. Nuclear Regulatory Commission have been served by the NRC internal mail system and others have been served by deposit in the U.S. Mail. One copy has been served on each person even though his or her name appears on more than one service list. In addition to copies served on Atomic Safety and Licensing Board and Atomic Safety and Licensing Appeal Board members identified on the service list, 19 copies of the attachment have been provided to the Atomic Safety and Licensing Board Panel, and 1 copy of the attachment has been provided to the Atomic Safety and Licensing Appeal Board Panel.



UNITED STATES
 NUCLEAR REGULATORY COMMISSION
 WASHINGTON, D. C. 20555

SEP 25 1978

MEMORANDUM FOR: Milton J. Grossman, Hearing Division Director and
 Chief Counsel, OELD

FROM: D. B. Vassallo, Assistant Director for Light Water
 Reactors, Division of Project Management, NRR

SUBJECT: BOARD NOTIFICATION - SEMISCALE EXPERIMENT S-A7-6
 (BN-78-17)

The enclosed staff memorandum discusses unanticipated results during recent semiscale tests and I think is self-explanatory in terms of information available to date.

Although the memorandum recommends notifying Boards following the availability of additional information and a more detailed staff assessment, I feel that the memorandum, as written, should be provided to appropriate PWR Boards at this time. We will provide the additional information and assessments as soon as they are available, but the enclosed memorandum will serve the purpose of alerting Boards of a potential problem.

Our list of PWR cases before Boards in the service list time frame is as follows:

Cherokee 1-3	North Anna 1	St. Lucie 2
Diablo Canyon 1-2	Pebble Springs 1-2	Three Mile Island 2
FNP	Perkins 1-3	Tyrone
Greene County	Pilgrim 2	Wolf Creek
Jamesport 1-2	Seabrook	WPPSS 4
Marble Hill 1-2	Shearon Harris 1-4	Yellow Creek
McGuire 1-2	Sterling	

A handwritten signature in cursive script, appearing to read "D. B. Vassallo".

D. B. Vassallo, Assistant Director
 for Light Water Reactors
 Division of Project Management

Enclosure:
 Memo, D. Ross to D. Vassallo
 dtd. 9/22/78 w/enclosures

cc w/enclosure:
 See page 2

Milton J. Grossman

SEP 25 1978

cc w/enclosure:

H. Denton
E. Case
J. Davis
R. Boyd
R. DeYoung
D. Eisenhut
T. Engelhardt
L. Nichols
B. Grimes
J. Stolz
R. Baer
O. Parr
S. Varga
IE (7)
D. Ross
R. Mattson
V. Stello
P. Check
T. Novak
Z. Rosztoczy
T. Murley
J. Scinto
S. Hanauer



UNITED STATES
 NUCLEAR REGULATORY COMMISSION
 WASHINGTON, D. C. 20555

SEP 22 1978

MEMORANDUM FOR: ✓ D. B. Vassallo, Assistant Director for LWRs, DPM
 FROM: D. F. Ross, Jr., Assistant Director for Reactor Safety, DSS
 SUBJECT: BOARD NOTIFICATION - RECENT SEMISCALE EXPERIMENT S-A7-6

Semiscale experiment Mod-3, S-A7-6 was run on September 12, 1978. It was intended to model an integral blowdown-refill-reflood scenario for a double-ended cold-leg break. On September 21, 1978 INEL staff provided for NRC a briefing of the results of the test.

Some of the results were unanticipated. For example, the heated core simulator was projected (by Semiscale) to quench at 110 seconds. Instead, it dried out again and went through several cycles of dryout and rewet (see enclosed Figure 1). Other portions of the cladding temperature showed similar discrepancies wherein test temperatures were somewhat below predicted (see Figure 2, 3). During the test the downcomer voided several times in the time span 100-400 seconds. This was not predicted (Figure 4 shows one such void).

During the periods of downcomer voiding there was also negative (downward) flow from the heater to the lower plenum.

A quick-look report on this experiment will be published about October 1, 1978.

The significance to safety, in the sense of NRR Office Letter No. 19 is in the phrase "whether this information could reasonably be regarded as putting a new or different light upon an issue before Boards or as raising a new issue". The information from the experiment is that nearly complete downcomer voiding occurred after downcomer fill. This is not predicted during EM-Appendix K applications. Also, typical Appendix K calculations do not show successive dryout and rewets over the extended reflood cycle.

The present judgment by INEL is that experimental atypicalities, in particular in the stored heat in the downcomer pipe and in the 1-D arrangement of the downcomer, have produced an atypical and unanticipated result. In the coming weeks we and INEL intend to further study the issue and find out answers for the questioned experimental atypicality as well as the questioned failure of RELAP to have anticipated the result.

In my judgment, based on the INEL presentation, this experiment does not put in a new or different light the concept of PWR bottom - flooding FCCS. Nevertheless, it does require us to get more information from a source external to the staff. It is of sufficient importance to seek further information, first from NRC contractors, and perhaps licensees and vendors in due course. In this event I conclude that it meets the notification test. In NRR Office Letter 19, Enclosure 1, page 6-7, I am supposed to provide you the following:

1. the item for notification;
2. considerations regarding relevancy and materiality;
3. statement on perceived significance; and,
4. relation to projects.

1. The item

This memo and the figures show that an integral experiment intended to simulate many of the PWR LOCA phenomena displayed several unanticipated expulsions of water from the downcomer during what was expected to be a tranquil reflood process.

2. Relevancy and Materiality

The experiment is relevant to all bottom-flooding PWRs. I presently doubt that it is material due to perceived atypicality.

3. Significance

Current staff positions on this subject are through approval of Appendix K models.

If we thought a new phenomenon was discovered, we would alter our staff positions on those models. Until the atypicality issue and the code predictability issue is better documented, we do not propose to reopen PWR vendor model approvals. This position is interim, and based on the expectation that the experiment is atypical and that proof will be available in the order of weeks.

4. Relation to Projects

This relates to PWRs in general.

As far as documentation is concerned, I believe it is preferable to distribute notification of the October 1 Quick-Look Report along with a more detailed staff assessment of relevancy, materiality, and significance.

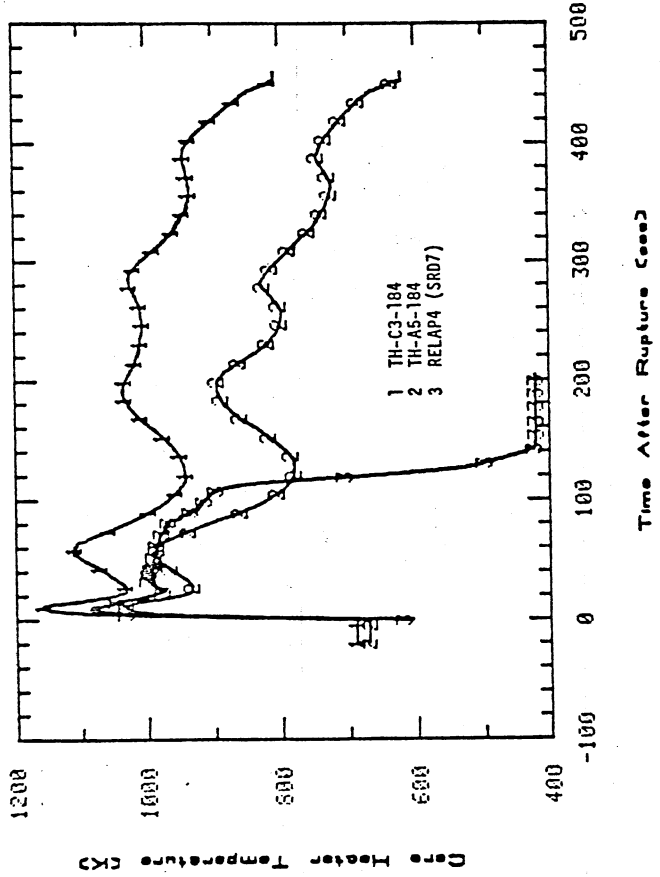
We could have this by October 15. If, however, more prompt notification is needed, this memo should suffice.

D.F.R.
D. F. Ross, Jr., Assistant Director
for Reactor Safety
Division of Systems Safety

Enclosures:
As stated

cc: R. Mattson
V. Stello
R. Boyd
D. Eisenhut
B. Grimes
P. Check
T. Novak
Z. Rosztoczy
T. Murley
J. Scinto
S. Hanauer

COMPARISON OF ROD CLADDING TEMPERATURES AT CORE HIGH
POWER ZONE WITH RELAP4 FOR TEST S-A7-6



COMPARISON OF MEASURED AND CALCULATED CLADDING TEMPERATURE
IN UPPER PART OF CORE FOR TEST S-A7-6

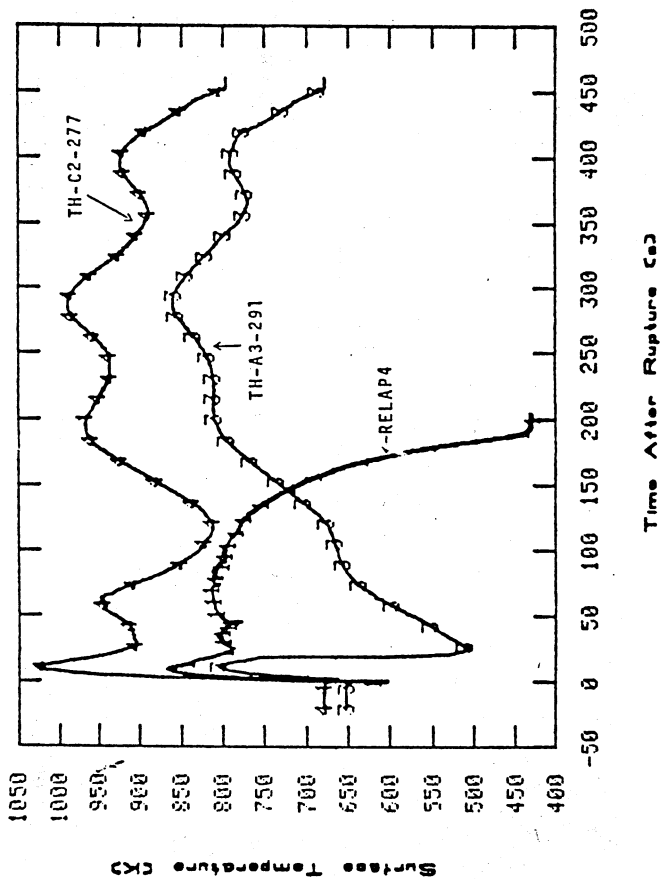


Figure 2

COMPARISON OF MEASURED AND CALCULATED CLADDING TEMPERATURE
IN LOWER PART OF CORE FOR TEST S-A7-6

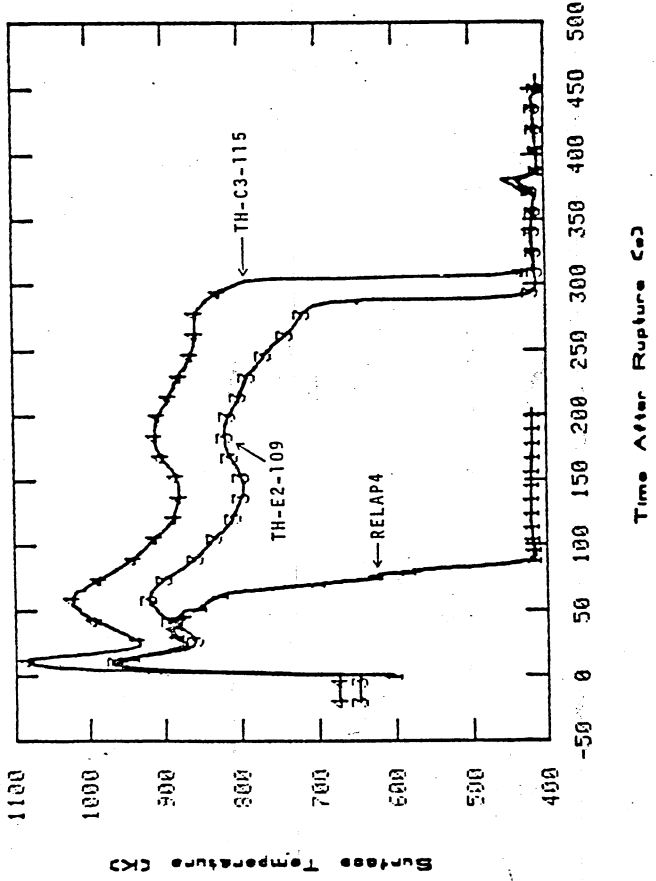
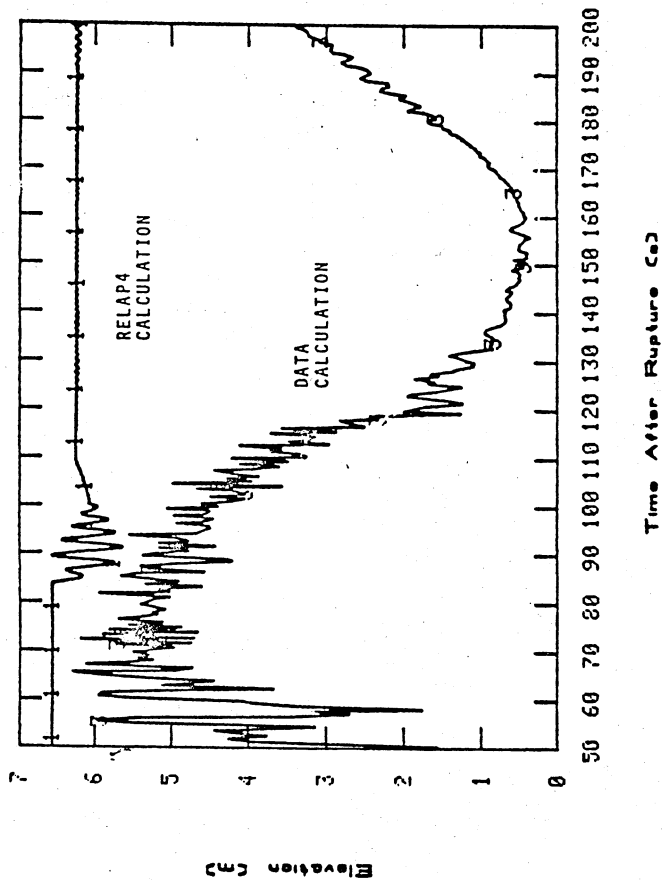


Figure 7

CALCULATED COLLAPSED DOWNCOMER LIQUID LEVEL FOR TEST S-A7-6



Attachment 4

ORNL-NSIC-24

Contract No. W-7405-eng-26

Nuclear Safety Information Center

EMERGENCY CORE-COOLING SYSTEMS FOR LIGHT-WATER-
COOLED POWER REACTORS

C. G. Lawson

OCTOBER 1968

OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee
operated by
UNION CARBIDE CORPORATION
for the
U.S. ATOMIC ENERGY COMMISSION

5. CONCLUSION AND RECOMMENDATIONS

The emergency core-cooling systems of several boiling- and pressurized-water reactors, were reviewed, the design basis and backup data were examined, and the need for certain additional data was established. Generally, the design approach used by the manufacturers is conservative when evaluating the energy released or the cladding temperature. Occasionally there is an absence of experimental data that is inconsistent with the apparent sophistication of the calculational procedures.

The following conclusions and recommendations are made as a result of this review.

5.1 Removal of Energy Sources

The emergency core-cooling system is an engineered safety feature designed to prevent a core thermal runaway by removing fission decay and stored energies and by preventing the release of potential energy in the Zircaloy-steam reaction. Lack of control and removal of these energy sources might lead to failure of the outer containment structure.

5.2 Damage to Core During Blowdown

The LOFT and the CSE programs are studying the blowdown of pressurized- and boiling-water reactors in detail. The questions relating to the mechanical integrity of the core and the piping have been defined and many can be resolved by the designers. The effect of pipe rupture propagation time and shock waves on the pressure loadings axially across the core and radially across the core barrel should be determined for short rupture times. The time to reach saturation pressure in the blowdown is about 0.05 sec for a large pipe rupture. Therefore even a propagation time of 0.01 sec is not considered an instantaneous break. Damage to the core internals during the depressurization may adversely affect the coolant distribution and core cooling during the blowdown and core re-flooding process.

The transient heat transfer from the fuel to the cladding to the coolant should be measured and understood for both pressurized- and boiling-water reactors during the quasi-steady-state blowdown. The fuel cooling rates during blowdown can influence by at least 1 min^{34} the minimum time required for water addition to prevent fuel cladding melting and/or excessive metal-water reaction. Core damage that would influence cooling rates should be prevented.

The LOFT and CSE programs are studying the amount of water remaining in the pressure vessel and high-pressure system after blowdown, since the water left in the reactor vessel affects both the time to reflood the core and the potential extent of the Zircaloy-steam reaction. Tests of the amount of water left in the vessel after blowdown have been extended to include determinations of the effect of core internals and the external piping on the amount of water left, since they may act as entrainment separators.

There are many computer programs and physical models available for calculating blowdown-pressure transients and water inventory. These computational methods are being tested by the LOFT and CSE programs. This effort should continue, since all these computer programs need normalization to data. Much time would be saved if the competence of the individuals from diverse organizations working on this effort was grouped to form a common source of information. Battelle Memorial Institute has recently initiated such a program at the suggestion of ORNL.

5.3 Spray Cooling of Core

Additional work is required to assure the reliability and effectiveness of spray cooling systems for the high specific power cores currently being designed, particularly for temperatures in the range 2000 to 2500°F. Extensive work by Phillips Petroleum Company is planned on Zircaloy rod bundles.

The data published by General Electric Company on the effectiveness of spraying 6×6 and 7×7 arrays of full-size stainless steel-clad fuel assemblies were obtained under conditions where the hottest fuel rod was assumed initially to be at 1800°F (representing some time after blowdown).

However, in their Browns Ferry reactor, for example, the calculated thermal condition of the core fuel rods 30 sec after the break when spraying was initiated would be as follows:

	Temperature	
	°C	°F
Hot spot	1177	2150
10% of cladding	>948	>1740
25% of cladding	>816	>1500
50% of cladding	>635	>1175

Some of the core would be at temperatures in the region where the metal-water reaction rate between Zircaloy and steam becomes significant. The experimental data clearly need to be extended to the temperatures of the accident.

Temperature distributions representing the consequences of moderate delays in initiation of emergency cooling should be simulated in some spray tests. Forced- and natural-convection heat transfer between steam and high-temperature Zircaloy should be measured and analyzed.

The gas pressure inside the fuel rods should be controlled at levels representative of reactor fuel to get a proper measure of the nature of the cladding failure as the blowdown occurs. The possibility that swelling of the cladding may cause blockage of the flow channel should be eliminated if gross swelling occurs. The relationship between the amount of steam-Zircaloy reaction and gas embrittlement should be determined. The condition leading to rod fragmentation upon quenching from high temperatures should be determined so that it can be avoided.

The possibilities of water-hammer formation by rapid addition of water to hot Zircaloy should be eliminated. The spray system relies on wetting the inside and outside of the fuel channel shroud and thereby presenting a radiation sink for the heat from the fuel rods. The Japanese and British data on the sputtering phenomenon, as well as the American work by General Nuclear Engineering Corporation on flooding of hot metal surfaces, show clearly that the time required for cooling and wetting a hot surface increases rapidly with increases in surface-to-steam temperature differences and decreases with system pressure. This influences the

lag time for rewetting the wall and fuel rods and requires that the rods be cooled by both thermal radiation to steam and steam convection until the walls are wetted. Tests should be run with hot fuel assemblies cooled by water at the temperature and pressure of the containment and pressure vessel environments following the accident and at heat fluxes corresponding to the newer BWR fuel designs.

5.4 Flooding or Immersion Cooling

The pressurized- and boiling-water reactors are cooled by a rising flood of water as an emergency coolant. The flooding systems are useful because they provide a uniform distribution of coolant. Current work at Phillips Petroleum Company at Idaho Falls in the FLECHT and SECHT programs is investigating the cooling characteristics of such systems. This work should be extended to parallel channels at different temperatures to assure that hot-channel starvation of coolant does not occur in shrouded channels.

The effects of boiling in open channels should be determined at cladding temperatures above 2200°F, since this may alter the required liquid level in the pressure vessel for adequate cooling in the postblow-down situation.

The use of the pressurized-water tanks on pressurized-water reactors is a practical solution to adding a large quantity of water to the core rapidly. The accumulators relieve the need of emergency core-cooling systems for almost-immediate pump power. These tanks should be designed so that the pressurized gas from the accumulator does not drive the water from the core after the initial injection.

Design efforts should continue on both PWR's and BWR's to decrease the response time of emergency core-cooling systems, since this may one day be the limiting factor on fuel specific power or on power density.

5.5 Structural Integrity of Core During Heatup

Some reactors still use stainless steel cladding on control plates and followers inside the hot region of the core. Since stainless steel

and Zircaloy react at temperatures below the melting point of stainless steel, this reaction should be explored to make certain it does not interfere with core cooling.

5.6 Structural Integrity of Vessel

The time required^{1,2} in a large-rupture loss-of-coolant accident for fuel that is unquenched to melt through the reactor vessel and possibly breach the outer containment vessel has been estimated at 1/2 to 1 hr. Therefore, a design and experimental effort should be initiated to arrive at a method of containing or stopping a vessel melt-through before the containment is breached in the event of the worst case of an inoperative emergency cooling system.

5.7 General Performance and Standards

The current reactor emergency core-cooling systems that reflood part of the core within 30 sec after a major break or which start adding coolant by spray distribution before the blowdown is complete appear capable of quenching the core and preventing a thermal runaway accident in which the core might melt down and penetrate the reactor vessel and containment shell. The emergency cooling system is an engineered safety feature of prime importance under some accident conditions in protecting the containment shell and controlling the radioactivity release from the fuel. Sufficient data should be obtained with heated Zircaloy-clad uranium dioxide fuel rods and water-steam mixtures to establish the physical phenomena that occur at temperature levels between 2000°F and the melting point of Zircaloy. Significant cladding swelling and cracking occur at temperatures from 1200 and 1800°F in all water-cooled reactors. The effect of these failures, if any, on flow channel blockage or flow distribution is not known.

Rapid activation of the emergency cooling system and long-term operation are the most urgent requirements in the event of a large-scale primary cooling system break. Therefore a continuing effort should be made to develop more rapidly acting systems with even better reliability than

systems currently being designed. To this end, systems tests that determine the effectiveness of the hardware acting in concert should be performed in environments designed to simulate an accident situation. There is no other certain demonstration of adequacy. These tests should be performed on a prototype of large scale. The revised LOFT programs²¹ may satisfy this need. The ability to predict system performance analytically could demonstrate an adequate level of understanding. Consideration of the improbable accidents (sabotage, earthquakes, falling airplanes, etc.) and the potential plant damage requires complete redundancy and protection of cooling systems in order to assure a working coolant-injection system in all circumstances.

Finally, the emergency provisions for a loss-of-coolant accident should be examined to determine that the provisions themselves do not create hazards. Specifically, the BWR automatic-relief system and the gas in the PWR water storage tanks could both worsen the situation by ejecting coolant from the core needlessly under certain circumstances.

5.8 System Tests

The accidents discussed in this report all lead to temperature, pressure, and humidity environments far different than those normally prevailing. Tests on the emergency cooling equipment for each reactor should be performed to supply assurance that hardware meets appropriate specifications and can survive and perform in accident situations and the resulting environments. Separate tests to (1) demonstrate hardware reliability and (2) system effectiveness may be sufficient. These are different from the prototype tests.

Maintenance and retesting of the emergency cooling system hardware, including power supplies, should be routine and sufficiently frequent to assure availability on demand.⁵⁷ Results of tests of emergency cooling systems for operating reactors show that emergency power supply availability can be improved by more thorough preventive maintenance.¹⁸

Frequent and routine tests of the availability of emergency equipment, such as are proposed in the preliminary design reports, should be carried out. The results of these tests should supply data that can

demonstrate the availability of equipment and the reliability to perform as designed by comparison with data obtained from the prototype tests proposed in Section 5.7.

5.9 Design Improvements

Efforts to improve the emergency cooling systems should be continued by design studies for reactors with higher specific power and flatter power distribution. Emergency cooling systems are designed to control the thermal and radioactive energy release from the fuel, limit the damage to the reactor complex, including the containment shells, and thereby help protect the public from gross exposure to radioactivity in the event of a primary coolant rupture and loss of power. The reactor operating variables of fuel specific power, plant thermal output, and to a lesser extent fuel burnup strongly influence economics as well as the emergency cooling system design requirements. The factors that improve economics also increase the demand on the cooling system pumps and power supply through increased demands on the time-to-startup margin and flow rates. The design studies would clarify specific future needs for the nuclear industry and the AEC.

The trend toward power flattening within the core of the next generation of water-cooled reactors requires more detailed knowledge of the water-steam-Zircaloy interaction to assess the details of the loss-of-coolant accident. An effort should be started soon to estimate the relationship between the power distribution within a large core, the maximum design cladding temperature in the postaccident situation, and the emergency cooling system design requirements in order to assess accurately the adequacy of the no-cladding-melting criteria or other criteria that may be suggested.

5.10 Priorities

All the items discussed above are of prime importance in assessing the safety of a reactor plant. In establishing priorities among the items for effort it is clear that those items that relate to future-generation plants or to plant maintenance may be given a lower priority than other items. However, all the questions should be answered before the newer plants have operated any appreciable time. No actual priorities may therefore be stated.

Mr. McCORMACK. Thank you, Dr. Kepford.

I want to remind the members that we are going to observe the 5-minute rule. I shall try to observe it as well as anyone, and ask all other members to do so, too.

I would like to direct my first question to Dr. Levenson, and to ask him—you said we have been unable to identify any new phenomena uncovered by the accident. Would that include the production of hydrogen in the reactor vessel itself?

Dr. LEVENSON. Yes; I think that is correct. The matter of the temperatures at which zirconium or its alloys, such as zircoloy, react with water to produce hydrogen is a well-established phenomenon.

The rates of reaction and the actual temperatures have been measured in the laboratories many times. The basic design of emergency core cooling systems is to keep zirconium metal below the temperature at which such a metal-water reaction occurs.

If you exceed that temperature, the reaction will occur. It is not a new phenomenon.

Mr. McCORMACK. Dr. Dietrich, I believe it was you who mentioned the necessity to be able to remove inert gases from the reactor. Would this be easily accomplished with existing powerplants? When they go down, could this be handled, to provide some method for venting reactors?

Dr. DIETRICH. I think it would be a fairly straightforward engineering job to do this, if one were interested only in the venting. But as I mentioned in my testimony, one has to give careful consideration to such changes. For example, it is another path for radioactivity to come from the primary system into the containment building. It is also another potential leakage path.

Mr. McCORMACK. What you are saying is it could be done?

Dr. DIETRICH. Absolutely, and it will be done, but I am only saying that we should not go out and say, OK, we are going to do it today, without giving it careful consideration and looking at the design—

Mr. McCORMACK. Any exhaust system would have to provide for the removal of fission product gases, traps, and scrubbers and so on.

Dr. DIETRICH. Right.

Mr. McCORMACK. You also mentioned on page 2:

To make less difficult demands on the operator and to be more forgiving of operator errors through minimization of the frequency of occurrence and speed of development of operation of perturbations with potential for hazard.

Are you suggesting that we should be building C-47's instead of P-51's here? In other words, are you saying that the plants are too hot to handle; that is, in the sense of being too hypersensitive to transients, and too fast for the operators to respond?

Dr. DIETRICH. No. But I think there are things that can be done. For example, I think the fact that the pressurizer appeared to be going solid, as they say, had a great deal to do with the Three Mile Island accident.

Maybe we need a somewhat larger pressurizer, so its volume is larger relative to the capacity of the primary system, so that it is not quite so sensitive. Or maybe we need a bigger inventory of

water in the secondary system, so that if the feed pumps go off, one is not immediately faced with the steam generators going dry.

Mr. McCORMACK. OK. Very quickly—

Dr. DIETRICH. It is engineering I am talking about.

Mr. McCORMACK. Let me ask you a couple of quick questions.

It would be relatively simple, wouldn't it, to install valve indicators on critical valves to tell what the valve is doing, as well as what it should be doing?

Dr. DIETRICH. I believe it would be relatively simple in principle. To actually go into the plant and do it would certainly take some time.

Mr. McCORMACK. Would it be your belief that we should go back and look at the design of some of the valves we have been taking from the shelf, and been using, such as pressure release valves, and explore their design, so that they could be made much more reliable?

Dr. DIETRICH. It is possible. I don't consider myself an expert on valves, but some of the things that we do in the name of safety perhaps haven't been as well thought through as they might be.

For example, now, the valve that stuck was the relief valve, whose purpose is really to keep the safety valve from opening. Since the safety valves are put on there, it is always a possibility that—

Mr. McCORMACK. But the release valve didn't close when it should.

Dr. DIETRICH. That is right. What I am saying is if the safety valve sticks open, there is no way to turn it off. There is no block valve. You are not allowed to put a block valve in because of the pressure codes.

Mr. McCORMACK. Wouldn't design and procedures allow you to have a control on the control panel that said open the valve, the valve is open, close the valve, the valve is closed?

Dr. DIETRICH. Oh, yes.

Mr. McCORMACK. OK. I don't have any more time. I have some more questions later on.

Mr. Goldwater?

Mr. GOLDWATER. Mr. Dietrich, I wonder if you could elaborate on a statement you made in your testimony, and I would be interested in Dr. Kepford's analysis of that elaboration. It is on the first page.

You say, "While the specific accident sequence was unforeseen, the engineered safeguards used were successful in protecting the public."

Dr. DIETRICH. Yes.

Mr. GOLDWATER. What do you mean by that?

Dr. DIETRICH. Well, very little radiation got out. One of the safeguards is the containment building. If you hadn't had that building there, you would really have been in bad shape. Eventually they did use the safety injection pumps to put water into the reactor. They are part of the engineered safeguards, also.

If they had not been there, or if they had failed to operate, you couldn't have recovered from the accident. These are the sorts of things I mean. The equipment was there. When it was turned on it worked.

Mr. GOLDWATER. Dr. Kepford, your allegation is that nothing worked.

Dr. KEPFORD. No; I didn't say that at all. I think probably much of the equipment worked as well as could be expected considering the designs and layout of the control room, and so on.

With regard to radioactive releases, from what I have been told by officials in State government, dozens of curies of radioactive iodine-131 were released, and millions of curies of noble gases.

This was a very major release of radioactivity. It was, I am sad to say, largely unmonitored. The largest releases of radiation went unnoticed.

At 7:30 Wednesday morning—the director of the Bureau of Radiological Health for the Commonwealth of Pennsylvania, Mr. Thomas Gerusky, told a public meeting in Newberrytown, Pa., a couple of weeks ago—the projected dose rate in Goldsboro was 10 roentgens per hour.

Now, the wind was heading right toward Goldsboro, from the plant. It is a very small town, a few hundred people, due west of Three Mile Island. Whether or not that dose ever got there, I don't know, but it certainly doesn't show up in any of the calculations or estimations of doses which have been released.

There was the release of gases March 30, Friday morning, headed off in the direction of Hershey, Pa. The dose rates were on the order of 100 millirems per hour projected.

But again, the monitoring was so bad that nobody was available to find out. When you look, for instance, between Three Mile Island unit 2 and that compass sector which includes Lancaster, Pa., one of the nearest large population centers, there wasn't a single radiation monitor, and so on.

So when people come by and say nobody was hurt from this accident and nobody was injured and the population exposures were very low, I think they are doing one of two things. They are either being very dishonest or they are relying on hopelessly incompetent monitoring. I don't think there is much of an excuse for either.

Mr. GOLDWATER. Dr. Levenson, as chairman of the Ad Hoc Industry Advisory Group that looked at this accident, do you have any comments?

Dr. LEVENSON. Our role did not include the health and safety monitoring, but I would comment in the context of Dr. Kepford's original statement that what is calculated is perhaps less reliable than what is experimental.

There were a lot of calculations made on projected doses, assuming both a level of release and a level of catastrophe that never occurred. We were directly involved only to the extent of monitoring at the site and close in to the plant as it affected the recovery operations.

Since nothing within orders of magnitude of this level was present at the plantsite, it is difficult to see how it could have been present miles away.

Regarding the question of what is adequate monitoring, with hindsight, like with most things, you never have enough data. But I think that in the data that exists, which came from multiple groups—there was not just one group doing monitoring—there is

indeed a very large discrepancy between what has been measured and what some people projected there might be. But this is not my field.

Mr. McCORMACK. Mr. Goldwater's time is up. It is Mr. Lujan's turn.

Mr. DORNAN. I wanted to ask a question out of sequence. I have some gasoline shortage experts in my office. We have two crises on each coast. But this is much more serious. I wanted to ask a followup question of Dr. Levenson, with a slight prolog.

Those of us who believe in nuclear energy, if we ever underestimate the impact on the public of the statements of Mr. Tom Hayden, his wife Jane Fonda, or the Dick Cavetts of the world, the Ralph Naders, we are making a big, big mistake to underestimate the impact they are having on the people.

Last night on television, on the Cavett show, Ralph Nader said he was just a little shocked about the timing of the Three Mile Island, that it was inevitable, that he expected a major accident to come closer to the year 2000.

But that given the inevitability of the growth of nuclear plants and the numbers involved, that it is just a matter of time and that he thinks the Three Mile Island incident is just that, an incident, and the major catastrophe is just to come.

The compelling part of his argument to the average American is there has not been a technological development anywhere where there has not been a catastrophe. For instance, the British Cunard lines built the unsinkable *Titanic*, and it goes down on its maiden voyage.

As a pilot, when I first saw the 747's, DC-10's, and 1011's take to the air, I thought, I wonder if we really have safety systems built in in such a way that there will never be an accident. But a Lockheed 1011 flies into the ground outside of Miami—pilot error.

A DC-10 loses a door off the rear over France, with a loss of life of over 340 people. Finally, a 747—I am not talking about terrorists, deliberate destruction—but a 747 crashes in Africa, killing a massive amount of people.

Now, Dr. Levenson, in the area of probability, if we weather this storm and nuclear plants continue to grow—and I am supporting them at this point—is Ralph Nader predicting, within the realm of probability, correctly when he says there eventually will be, just by the law of averages, a serious meltdown and a great loss of life?

This is disregarding the gentleman's figures on page 12, Dr. Kepford, that he believes hundreds, maybe thousands, will die already because of Three Mile Island.

Could you please project your thinking into the future, on the law of probability?

Dr. LEVENSON. Well, I am not an expert on the law of probability, and even less of an expert on public opinion, and how it is influenced. Fairly clearly it is not influenced by technical facts very much.

The matter of the type of accident and its consequences is basically about what we are talking. Incidentally, I disagree with Mr. Nader. Three Mile Island was not merely an incident, it was an accident. Anybody trying to say it wasn't an accident is playing games with words.

It was an accident, and it was a pretty serious accident. It was not catastrophic to public health. Most of the catastrophic accidents are invented by computers. They are not the result of any experimental or factual evidence.

As early as 1953, back in the early days of the AEC, reactors were pushed to destruction in Idaho, in the so-called Borax experiments, where reactors were actually destroyed to get evidence about what happens.

We have a very large amount of evidence from, reactor meltdowns. The first breeder reactor in this country, EBR-1, had a meltdown that destroyed two-thirds of its core. The SL-1, the first military so-called hotrod type of reactor, that resulted in the death of three men represented a destruction by meltdown and vaporization of a significant fraction of the core.

There was also the Fermi reactor. A large number of military accidents have occurred, including bombers, which were carrying plutonium warheads which crashed, where the plane went up in fire and everything else with it.

There have been many classified experiments in Nevada in the weapons program. A very large discrepancy exists between the theoretical projections of catastrophe and what the experimental evidence indicates.

The probability is such that eventually there will be more accidents and that some will be more serious than Three Mile Island. You must compare, from the total public risk standpoint, the number of people killed by various sources of generating electricity. It must be on this basis—you cannot say if nuclear power kills 100 people once every 5 years, we don't want it, if the alternatives kill 10 times that many people.

It is comparative risk analysis that is conspicuously absent in the statements that you have quoted.

There probably will never be an accident absolutely identical to Three Mile Island. Probably there will be some similar accidents, and there probably will be some even more severe. I just don't think there will be any that we could truly call a major catastrophe.

If you want to use your analogy of aircraft, we have yet to worry about either a DC-10 or a 747 reaching escape velocity and taking its passengers out into deep space. Equally improbable questions are being asked about nuclear power.

Mr. McCORMACK. Will the gentleman yield?

I think there is one portion of the question and answer that needs just one additional bit of clarification. I would like to ask Mr. Levenson to answer it; that is, it is not necessary that anyone be harmed in the event of a meltdown.

One could have a meltdown without harming anybody, even inside a plant. You can have a complete meltdown and no one will be harmed inside a plant, is that correct?

Dr. LEVENSON. That is correct. We have already had a number of experimental and accidental meltdowns. The function of the containment building and all of the auxiliary systems that are in it is to handle such meltdowns—the recombiners dispose of hydrogen if it is generated, et cetera.

There isn't any indication from factual experience that even a meltdown automatically leads to the catastrophic consequences that is talked about.

Mr. McCORMACK. Thank you.

Now, did the gentleman from New Mexico wish to yield any more time to the gentleman from California?

Mr. GOLDWATER. I will yield the full 5 minutes to the gentleman from New Mexico.

Mr. LUJAN. I thank the gentleman. I don't think I need 5 minutes. Looking over all of the testimony, it seems to indicate, except for Dr. Kepford's, that we ought to concentrate on stopping the small accidents, and that if we do that, that the big accidents will take care of themselves.

Maybe not quite as simple as that, but that the priority ought to be on those small accidents.

Would you care to enlarge on that? Have I gathered at least the feeling of what the testimony was about? Any of you?

Mr. KENNEDY. The answer to your question is yes. The large accident has been pretty thoroughly studied. I personally believe that if one builds a reliable powerplant, it will also be a safe powerplant. That doesn't mean the thing should be ignored, but we spend a tremendous amount of time on the very large accident and not enough on the reliability.

Mr. LUJAN. The sequence of events at Three Mile Island shows that within 3 hours, at a time somewhere about 2¾ hours, something like that, there were some 50 or 60 people running around inside the control room.

It leads one to believe that there was just utter confusion in that control room. Maybe my interpretation of it is a little exaggerated, but if that were the case—I have been in that control room—there were just about a dozen of us there at the time, and it certainly was crowded.

Because accidents happen with some frequency, is there any group, like a SWAT team of some kind, some group that is put together from laboratories, from industry, from wherever it may be, that can come in, and take control of a dangerous situation, and bring it under control?

Is there anything like that? If there isn't, should there be something like police SWAT teams to respond to those situations?

Dr. DIETRICH. I can say that as far as my company is concerned we have set up teams of this sort since Three Mile Island. So we have taken action on something we learned. But of course there is no way that we can set it up to use people other than our own.

But they are very knowledgeable people. These teams include people who have been our representatives during startup of plants and that sort of thing.

So that they are not by any means just theoretical people. They are people who know how to press the buttons and work the valves.

Mr. LUJAN. These are trained only in your type of reactors. In other words, they would have no knowledge about reactors designed and built by somebody else.

Dr. DIETRICH. I think they would be helpful, but of course it would probably be more effective if each manufacturer—

Mr. LUJAN. How would each company feel separately about standardization? It just seems to me—I am not an engineer—that if we had standardized design and construction of plants, that it would make it so much easier.

Now, would you submit to a group type of design and construction, or do you think yours is that much better, that maybe you wouldn't want to be dropped into a standardized group?

Dr. DIETRICH. Well, I am not really sure how one might implement such a thing.

Mr. LUJAN. You design a powerplant, you say this is really the way a powerplant ought to be, this is the standard model, it will have all of the things that you have been talking about, it is earthquake resistant, the valves are good, the pumps are good, all of the different components are good.

Therefore, this is the plant that we would build. All we have to do is the foundations, build them up.

Dr. DIETRICH. I think that is essentially what I was speaking of in the program that we were recommending. But I did not say to come up with a single design.

Mr. LUJAN. Why not?

Dr. DIETRICH. Because I just don't know how to do it. I mean, I don't know how to implement it. Now, I am not saying there is not a way of doing it. It is just not my field. It would get pretty complicated on things like antitrust.

Mr. LUJAN. On the contrary, it seems to me—even though my time is up—that on the contrary, it would make it so much easier. Here is my powerplant, you go to the NRC, they say, yes, we know all about this plant, and they give you a license.

Dr. DIETRICH. I cannot really speak for my company. I would guess my company would certainly participate in such a thing, if there were such a thing.

Mr. McCORMACK. I thank the gentleman from New Mexico. The gentleman from Pennsylvania, Mr. Walker.

Mr. WALKER. Thank you, Mr. Chairman.

I have questions of a couple of people. So I hope maybe they can be as brief as possible with their answers.

Mr. Levenson, in your testimony, I kind of read between the lines that you are saying that perhaps the regulators and the regulated have gotten a little too cozy on this business of watchfulness over plant design and public safety.

Is that a fair assumption that I have drawn from what you had to say?

Dr. LEVENSON. No; I don't think there is a coziness at all. What I am saying is that the people applying for licenses are reacting to the pressures from the regulators, and that if everybody is preoccupied with the wrong thing, it doesn't matter how cozy or how antagonistic they are, you don't address the really significant questions.

Mr. WALKER. When you took a look at the situation at Three Mile Island, did it occur to you that perhaps there was kind of cozy relationship, in the initial licensing procedure, the initial procedure that brought it on line, to come in under the December 31 date for licensing?

Dr. LEVENSON. I have reviewed none of the records and none of the proceedings or testimony for the licensing, so I cannot comment on that.

Mr. WALKER. OK.

You make a statement here in your remarks that the confirmatory message of Three Mile Island is that we must go back and assure ourselves that we are doing everything that is practicable to reduce the risk to the public and to the plant.

I am particularly interested in the public. What is the nuclear industry doing now that Met Ed wants to dump that radioactive waste water into the Susquehanna River? Wouldn't it be wise for the industry to be coming down on the side of doing their very best to protect the public in this aftermath of Three Mile Island?

Dr. LEVENSON. I am not aware of any proposal to dump radioactive water into the river. I think there is a proposal that after the water has been decontaminated, that the cleaned up water be dumped into the river.

That is quite different than dumping the radioactive water.

Mr. WALKER. It will still have low levels of radioactivity in it, wouldn't it?

Dr. LEVENSON. Everything in the world is radioactive. I have been involved in many cases where the problems were that radioactivity in river water that we pumped out for cooling water was greater than the allowable standards to put it back into the river. One has to ask how radioactive, what are the standards.

I don't know of any request for an exemption from what are considered acceptable standards.

Mr. WALKER. I say to you that the public up there is extremely concerned about dumping that water, and whether or not it meets specific tests and so on. I think the industry, if they are really concerned about the risk to the public over the long term, ought to look into that.

Dr. Kefford, I would like to follow up on a couple of statements you made as well. You made the statement that you felt that the NRC lied along the way on this. Do you include Dr. Denton's statements in the fact that NRC was lying to the people of the area?

Dr. KEFFORD. I don't know which particular statements you are referring to.

Mr. WALKER. Well, in general I think the public accepted much of what Dr. Denton had to say. Was he lying along the way?

Dr. KEFFORD. I don't believe so.

Mr. WALKER. OK. Fine.

You are making the point that the monitoring of the radiation was not very good.

Dr. KEFFORD. It was abominable.

Mr. WALKER. I think you said radiation monitors only went out 13 miles.

Dr. KEFFORD. The NRC's only went out 13.8 miles, that is correct.

Mr. WALKER. I am a little bit confused, then. The studies on which all the calculations have been made on sites that go out as far as Reading, which is considerably further out than 13 miles.

Now, all of the studies, all the health effects are out at least that far, Reading, Carlisle, all of the areas had dosimetry monitoring in them.

Are you saying that—

Dr. KEPFORD. They are not mentioned in the reports that I have seen.

Mr. WALKER. They are part of the health effects study. That is the NRC study—which says that only one or two people will die as a result—of TMI. Those were the dosimetry sites that they used. That is in direct contrast to your statement here that hundreds and thousands are going to die.

I mean, these are my neighbors we are talking about.

Dr. KEPFORD. I am aware of that. This is the report that I am talking about. You can have it if you want. But measured radiation readings, elevated readings in Reading are not mentioned.

Mr. WALKER. I am talking about the Population Dose and Health Impact of the Accident at Three Mile Island nuclear station.

Dr. KEPFORD. May 10?

Mr. WALKER. Yes. The dosimetry sites in there include Lebanon, Reading, Lancaster, Harrisburg, Carlisle, York, and so on, most of which are further out than 13 miles.

Dr. KEPFORD. Where are you reading this?

Mr. WALKER. I am back on page 20, where I have the location of the dosimetry sites. It is my understanding that all of those sites were used as a part of the data base.

Dr. KEPFORD. On that map, the only sites that have dosimeters on, for instance, near Harrisburg, 15-G-1, is a dosimeter site. There is one south toward Lancaster, but only about 14 miles from the plant. That is 7-G-1. Closer in is 7-F-1. South of York is 9-G-1. I think those are the only dosimeter sites there.

Mr. WALKER. I was under the impression that the sites also marked at Reading, Lancaster, and so on are also dosimeter sites.

Dr. KEPFORD. I am sorry. I was unaware of that.

Mr. WALKER. That is my impression. I will have to go back and check it. That was my impression of the data.

Dr. KEPFORD. The data in here that I have looked at has only been the NRC data. The Met Ed data has been too scattered for me to do anything with.

But in a lot of directions, as you go away from that plant, the dose does not fall off with distance. In fact, in some cases it increases with distance. This, in my mind, tells me that neither NRC nor Met Ed had the slightest understanding of what the weather conditions were like, first off, in the lower Susquehanna River valley and secondly in that first week of the accident; that is, there was a relatively static air mass over that area, and the radioactive materials that were released simply did not normally form a plume and dissipate and blow over to somewhere else like they normally do.

They were held down by a temperature inversion and slid up and down the Susquehanna River, and off into the surrounding communities.

Mr. WALKER. I was out and did a little bit of the monitoring with them when I was on the site. I know they went down river with portable monitors a good deal further than what would be indicat-

ed as close in monitoring because I was along when they were doing some of that.

I assume some of that data got in. If I could, Mr. Chairman, just one last question.

The thing that disturbs me is that you use the figure hundreds and maybe thousands, that you believe are going to die. Those are the kinds of things that make good print in newspaper articles and so on, those kinds of figures.

Yet you are, it seems to me, a little bit guilty of the same thing you are accusing the industry of being. You say you can't quantify the number. Yet you come back and say the main problem with the industry is the fact that the industry doesn't have exact experiments to show what is going to happen.

When you use figures, it seems to me you are using them for political kinds of purposes.

Dr. KEPFORD. This again, Congressman Walker, was another experiment that was carried out on human beings, where nobody was around to collect the data. It is not my responsibility to collect the data. The NRC and Met Ed and those responsible are supposed to be doing that.

What I was saying was that their treatment of the data in my opinion, the NRC data, is dishonest. That is what I am saying. I did a very quick estimation. It could be high, it could be low by a factor of two on the person rem exposure.

In here they quote 3,500. I came up with 57,000. That is quite a difference. That suggests to me that the data was simply handled wrong.

I would be very glad to go over this with you in person, or go over it here, what I did with the data.

Mr. WALKER. But the fact remains that your testimony says, "I cannot quantify the number exactly, but I have reason to believe that the number may be in the hundreds or in the thousands."

What I am saying to you is that is exactly the same thing that—

Dr. KEPFORD. Can I go on. This is based partly on the statement of others, including none other than Karl Z. Morgan, who is well known, I am sure, to members of this committee, who stated at the Village Voice teach-in a week ago Saturday that he believed somewhere between 60 and 120 people, I believe, would die from this accident.

Mr. McCORMACK. I think we are going to have to terminate this part of the testimony here, Dr. Kepford. Our time is up on it. We are going to have to get on to the next panel because we have to adjourn by 12:00.

I am sure that the witnesses will be willing to answer further questions in writing for many of the members of the committee. I want to thank them.

I do think there is one thing to be pointed out here; that is—Congressman Walker would be particularly interested in this, and I don't know whether you have done this calculation—based on the cancer deaths in this country, the normal cancer rates, of the 800,000 cancer deaths in this area around Pennsylvania from normal causes; that is, there are 400,000 cancer deaths in this

country per year today, and over the next 20 years there will be 8 million cancer deaths in this country.

Of that—I beg your pardon. There will be 80,000 cancer deaths in that same population, in the next 20 years. If the NRC report is correct, if it is correct that the average individual dose they quote is 1.5 millirems, then from background it would be 100 times that much. From normal background, and whatever cancer deaths are suggested from the accident, if the NRC figure is correct, then the deaths from background would be 100 times, during this same period, for any one year.

Mr. WALKER. I thank the chairman for that. I think one of the worries of the community up there is how much we are beginning to build up when we start dumping the waste water into the Susquehanna, and how much you build on top of that. It is one of the real concerns.

Mr. McCORMACK. I think the concern the gentleman has is very well taken. I think it is a question that we should address to the NRC tomorrow, whether the radiation level of the water released, proposed to be released at Three Mile Island is above or below background, and if so, how much, so we can get some feel for that. That would help you and your constituents.

I want to thank the gentleman of the panel very much for appearing today. You are very kind.

We have one more panel at this time. The next witnesses are Mr. Saul Levine, Director of the Office of Nuclear Regulatory Research for the Nuclear Regulatory Commission, and Dr. Harold Lewis, professor of physics for the University of California.

These witnesses can provide us with exceptionally valuable testimony.

Dr. Lewis, do you want to come up and join us at this time. We welcome you.

STATEMENT OF SAUL LEVINE, DIRECTOR, OFFICE OF NUCLEAR REGULATORY RESEARCH, NUCLEAR REGULATORY COMMISSION

Mr. McCORMACK. By way of background, and for a better understanding by the members of the committee, Dr. Levine was very active in the preparation of what is known as the Rasmussen report, WASH-1400, in which an attempt was made to quantify the potential for nuclear accidents involving deaths of individuals.

Dr. Harold Lewis headed up a group that provided some extremely responsible, constructive criticism, at a later date, of the Rasmussen report.

Unfortunately, the press seriously distorted the intent of the Lewis review of the Rasmussen report and took advantage of what was perhaps some unfortunate language in the statement of the Nuclear Regulatory Commission in evaluating and accepting the Lewis report. In the press, it appeared that NRC was rejecting the Rasmussen report and as if the Lewis study constituted total rejection of the Rasmussen report.

All those involved know this was not the case, but it is important today for the general background of the Members of Congress to help bring this point out, and to help give us some perspective with respect to the safety design philosophy of nuclear powerplants, and

the implications of the Three Mile Island accident with respect to nuclear safety in general.

Then in addition to that, Dr. Lewis will be testifying on the general safety and statistical analysis of the hazards associated with nuclear powerplants and his report that he made previously.

So we are looking forward to this testimony. First of all, the statements of both you gentlemen will without objection be inserted in the record in their entirety and you gentlemen may proceed as you wish.

Mr. Levine, would you care to go first?

Mr. LEVINE. Thank you, sir.

I have a brief oral statement to make, Mr. Chairman, which I hope will be adequate for your purposes. I will cover three subjects, sir—the safety design philosophy for nuclear powerplants, the relationship between the Three Mile Island accident and the reactor safety study and the lessons we have learned from Three Mile Island about additional research needed on the safety of nuclear powerplants.

First, nuclear powerplant safety design philosophy.

In approaching the safety design for nuclear powerplants, the NRC recognizes that these plants present some potential for accidents that can have large consequences.

Because of this, we also recognize the need for a comprehensive regulatory process to help insure that no undue risk to the health and safety of the public will arise from their operation.

This process involves a well-developed safety design approach, the specification of safety design requirements to implement that approach, and an extensive safety review and licensing process to ensure that plants meet established safety requirements.

A key element behind these requirements and procedures is a recognition of the need for redundancy not only in the elements of plant design but also in the review process.

The need for redundancy derives from the understanding that in spite of man's best efforts to achieve high quality in design, construction, and operation of nuclear powerplants, these goals cannot be achieved; that is to say, no body of knowledge can ever be complete enough to reduce uncertainties and risks to zero.

The safety design approach used by the NRC emphasizes defense in depth. In nuclear powerplants, a series of physical barriers is constructed between the large amounts of radioactivity contained in the nuclear fuel and the environment.

Since it is known that some types of failures in one of these barriers can also cause failure of the other barriers, there are two other important factors involved in the implementation of the defense-in-depth approach.

These are, first, the specification of requirements to achieve high quality in the design, construction, and operation of nuclear powerplants to reduce the likelihood of failures that could potentially cause accidents; and second, the use of engineered safety systems, with redundancy when needed, to prevent failures from progressing into accidents.

These requirements are outlined in NRC regulations, standards and safety guides which are based on sound engineering practices established over the past 20 years, and which are undergoing con-

tinuing improvement. The NRC also sponsors a comprehensive research program to provide the technical bases for the confirmation of NRC's safety decisions and for needed improvements.

In summary, I believe that while nuclear powerplants, or any other of man's technological endeavors, cannot achieve risk free operation, the current system has provided a sound basis to ensure that nuclear powerplants present no undue risk to the health and safety of the public.

Of course, we have learned lessons from Three Mile Island, and have to do some work, which I will come to later in my testimony.

I would like to say a few words about the Three Mile Island accident and its relationship to the reactor safety study, WASH-1400. The comments I will make here should be regarded as preliminary because although we understand the basic elements of the TMI event, there are many details yet to be filled in.

From the viewpoint of nuclear powerplant safety design, two principal technical elements are involved in TMI. The most important is that the plant was configured so that the pressure relief valve on the primary coolant system opened very often due to events such as a failure of normal feedwater flow to the reactor.

An important matter in TMI and similar plants is to reduce the frequency of opening relief valves since, if the valves do not open, they cannot stick open and cause a small loss-of-coolant accident (LOCA), as apparently happened at TMI. This has been addressed in the bulletins issued by the NRC which require such actions as the installation of anticipatory signals that would result in earlier plant shutdown, raising the pressure setting at which the relief valve would open, and reducing the pressure at which the reactor is signaled to shutdown. These changes should, in principle, significantly reduce the likelihood of the valve opening.

The second area relates to the reliability of the auxiliary feedwater system. The question of interest is whether the RSS correctly predicted the chance of failure of the auxiliary feedwater system to operate when needed. Certainly the RSS identified that the system could be failed because the output valves of the system would be incorrectly left closed after maintenance, as was done at TMI.

The incident at TMI does not give us data as a failure point, because the system did perform its intended function although only after 8 minutes into the accident. However, it was a precursor to possible failure and this suggests that we will have to go back and reexamine the RSS predicted failure likelihood for this system to see if changes are needed.

The TMI accident has also indicated areas requiring additional safety research information.

While some of these requirements can be accommodated by reprogramming and reorientation of ongoing efforts, we believe there will be a significant amount of new work that will require resources over and above those contained in our fiscal year 1980 budget request to the Congress.

Therefore, we are currently preparing a proposed fiscal year 1980 supplemental budget request for review by our Commission. While I can indicate now the areas in which I believe research will be needed, I cannot go into great detail because we are still developing this information. However, I can indicate that our research needs

are generally greater in the study of accidents which can lead to extreme core damage, but which would fall short of actual melting of the core.

So far my examination of the TMI accident suggests that research is needed both to reduce the likelihood of events of this type and to obtain a better physical understanding of them. As I said earlier, additional resources will be needed to accomplish this work. The following topics need urgent attention:

A. TRANSIENT AND SMALL LOCA EVENTS

Ongoing research efforts must be accelerated to obtain engineering data on behavior of the fuel, the release of fission products from the fuel, and the thermal hydraulic behavior of the core and primary coolant system during transient and small LOCA events. These data are required to accelerate development and testing of analytical models and computer codes needed to give more precise predictions of actual system performance.

B. ENHANCED OPERATOR CAPABILITY

The accident at Three Mile Island has also demonstrated the urgent need for system improvements to enhance in-plant accident responses. This area of research need was given high priority and addressed in some detail in the NRC's "Plan for Research to Improve the Safety of Light-Water Nuclear Power Plants" (NUREG-0438), submitted to the Congress in April 1978. This work, which needs to be accelerated, includes improved data display and diagnostic systems to assist the plant operator under accident conditions, additional in-vessel and plant instrumentation which will operate reliably under such conditions, enhanced data transmission capabilities to obtain outside assistance during emergencies, system interlocks to preclude plant operation unless all safety systems are in an operable condition, and development of improved requirements for operator training simulators.

C. PLANT RESPONSE UNDER ACCIDENT CONDITIONS

Research is required to explore more fully the response of plant safety systems and components during accident conditions in order to understand better the physical processes that can occur so as to help preclude further system failures. Efforts in this area include a detailed understanding of the primary coolant chemistry following fuel failure, hydrogen evolution and behavior in the primary system and containment, and behavior of safety components of the plant, that is, reactor vessel pumps, valves, et cetera, under prolonged accident environments.

D. POSTMORTEM EXAMINATION AND PLANT RECOVERY

It is apparent that significant postmortem examination of the TMI core, plant components and the containment will be very useful in obtaining necessary information on fuel behavior, fission product transport and plateout and component operability under prolonged accident environments. These examinations will also be necessary to help define plant recovery requirements and risks.

The TMI core must be removed from the reactor vessel in a manner such that important configuration information is not lost. The core should then be shipped to appropriate hot cell facilities where it can be examined and analyzed extensively. These studies will provide significant data on coolability of damaged cores, fuel/clad/coolant interactions, and fuel chemistry under severe heatup conditions.

I hope that the views I have expressed here today regarding the safety design philosophy for nuclear power plants and the Three Mile Island accident, including the lessons to be learned from TMI as they relate to our research needs, will be of value to the committee in its considerations of these important issues. I believe significant regulatory actions are already underway to reduce the likelihood of such incidents significantly. For the longer term, I am sure that further improvements will also be effected. The research areas I have mentioned above should be started soon to provide the needed information.

Thank you, Mr. Chairman.

[The prepared statement of Saul Levine follows:]

STATEMENT OF SAUL LEVINE, DIRECTOR
OFFICE OF NUCLEAR REGULATORY RESEARCH, NRC
BEFORE THE SUBCOMMITTEE ON ENERGY RESEARCH AND PRODUCTION
May 22, 1979

Introduction

Mr. Chairman,

I am pleased to be here today to give you my views on the safety design philosophy for nuclear power plants, relationship between the Three Mile Island (TMI) accident and the Reactor Safety Study (RSS), and the lessons we have learned from the Three Mile Island event about additional research needed on the safety of nuclear power plants. While the Three Mile Island accident was indeed a highly regrettable event, it does give us an opportunity to learn some lessons needed to prevent instances of this type in the future and thus enhance the safety of nuclear power plants.

Nuclear Power Plant Safety Design Philosophy

In approaching the safety design for nuclear power plants, the NRC recognizes that these plants present some potential for accidents that can have large public consequences. Because of this, it also recognizes the need for a comprehensive regulatory process to help ensure that no undue risk to the health and safety of the public will arise from their operation.

This process involves a well developed safety design approach, the specification of safety design requirements to implement that approach, and an extensive safety review and licensing process to ensure that plants meet established safety requirements. A key element behind these requirements and procedures is a recognition of the need for redundancy

not only in the elements of plant design but also in the review process. The need for redundancy derives from the understanding that, in spite of man's best efforts to achieve high quality in design, construction and operation of nuclear power plants, these goals cannot be completely achieved; that is to say, no body of knowledge can ever be complete enough to reduce uncertainties and risks to zero.

NRC's regulatory process has relied and will continue to rely on the judgment of highly skilled engineers and scientists as the principal basis for its safety decisions. While extensive strides have been made in the development of quantitative risk assessment techniques, and the careful use of such techniques can provide added engineering insights about the safety of nuclear power plants, they have so far been developed only to the point where they can provide a valuable supplement to the other methods and procedures now used by the NRC to form its safety judgments.

The safety design approach used by the NRC emphasizes defense in depth. In nuclear power plants, a series of physical barriers is constructed between the large amounts of radioactivity contained in the nuclear fuel and the environment. The fuel is contained in a sealed metal cladding; the clad fuel is contained in a sealed, steel primary coolant system; and the primary coolant system is enclosed in a sealable containment building. Since it is known that some types of failures in one of these

barriers can also cause failure of the other barriers, there are two other important factors involved in the implementation of the defense in depth approach. These are, first, the specification of requirements to achieve high quality in the design, construction and operation of nuclear power plants to reduce the likelihood of failures that could potentially cause accidents; and, second, the use of engineered safety systems, with redundancy when needed, to prevent failures from progressing into accidents. These requirements are outlined in NRC regulations, standards and safety guides which are based on sound engineering practices established over the past 20 years, and which are undergoing continuing improvement. The NRC also sponsors a comprehensive research program to provide the technical bases for the confirmation of NRC's safety decisions and for needed improvements.

The NRC's regulatory process for nuclear power plants consists of safety reviews by the staff of the Office of Nuclear Reactor Regulation and by the statutorily independent Advisory Committee on Reactor Safeguards. Public hearings of the results of the staff and ACRS reviews are held by an NRC Atomic Safety and Licensing Board. The results of these hearings can be appealed to an NRC Appeals Board and the Commission. Beyond this, appeals can also be made to the courts. These reviews are conducted twice--once before the construction of a plant is allowed to commence and again before operation of the plant is permitted. The reviews also include environmental as well as health and safety considerations.

The NRC's Office of Inspection and Enforcement conducts inspections during construction of the plant to help ensure that the plant is being built in accordance with the safety design and quality requirements. Inspections are continued during the operating life of the plant to help ensure that the requirements of NRC's licenses are adequately enforced, that problems arising in operation are well handled, and valuable feedback from operating experiences is incorporated into the safety reviews of additional plants. Furthermore, NRC licenses require utilities to test important safety systems periodically and to report failures of all safety related equipment to the NRC. The results of NRC inspections and reports of equipment failures are routinely made public.

In summary, I believe that, while nuclear power plants (or any other of man's technological endeavors) cannot achieve risk free operation, the current system has provided a sound basis to ensure that nuclear power plants present no undue risk to the health and safety of the public.

THREE MILE ISLAND AND THE REACTOR SAFETY STUDY

I would like to say a few words about the Three Mile Island (TMI) accident and its relationship to the Reactor Safety Study (WASH-1400) which is more commonly called the Rasmussen Report after Professor Norman C. Rasmussen of the Massachusetts Institute of Technology, who directed the

work. The comments I will make here should be regarded as preliminary, because although we understand the basic elements of the TMI event, there are many details yet to be filled in.

From the viewpoint of nuclear power plant safety design, two principal technical elements are involved in TMI. The most important is that the plant was configured so that the pressure relief valve on the primary coolant system opened very often due to events such as a failure of normal feedwater flow to the reactor. The second relates to the reliability of the auxiliary feedwater system which is needed to remove the heat from the reactor after it has been shut down.

For the PWR studies in the Reactor Safety Study (RSS) as well as for most other PWR's, the primary coolant system pressure relief valve would not be expected to open in the event of failure of the normal feedwater system. The difference between those plants and TMI would be that they would automatically be shut down quickly when normal feedwater flow stopped, thus rapidly reducing the amount of heat that had to be dissipated and causing only a small rise in reactor system pressure. In the TMI accident the loss of normal feedwater, in and of itself, caused the relief valve to open very quickly (in 3 seconds). If this valve were to stick open, and valves of this type have about one chance in fifty of doing so, the plant would experience the equivalent of a small Loss of Coolant Accident (LOCA)*. This is what happened at the Three Mile Island plant.

*Attachment I hereto contains a description of a Loss of Coolant Accident

Thus, an important matter in TMI and similar plants is to reduce the frequency of opening relief valves since, if the valves do not open, they cannot stick open and cause a small LOCA. This has been addressed in the bulletins issued by the NRC which require such actions as the installation of anticipatory signals that would result in earlier plant shutdown, raising the pressure setting for opening of the relief valve and reducing the pressure at which the reactor is signalled to shutdown. These changes should, in principle, significantly reduce the likelihood of the valve opening.

The second area relates to the reliability of the auxiliary feedwater system. As pointed out in the RSS, the lack of availability of both normal and auxiliary feedwater systems can lead to serious overheating and melting of the nuclear fuel. Although this type of sequence was one that contributed significantly to the accident risks predicted in the RSS, the auxiliary feedwater system analyzed in the RSS was found to be a highly reliable system. At TMI, the auxiliary feedwater did not fail permanently; it was out of operation for only the first 8 minutes of the accident, after which it functioned properly. Plant temperature data indicate that this did not affect the course of the accident significantly; and, although it may have served as a source of distraction to the plant operator, the system basically performed its design function.

The question of interest is whether the RSS correctly predicted the chance of failure of the auxiliary feedwater system to operate when needed. Certainly the RSS identified that the system could be failed because the output valves of the system would be incorrectly left closed after maintenance, as was done at TMI. In most reactors, even if this were to happen, there would be 30 to 60 minutes available for the operator to correct the situation before any fuel damage would be expected to occur. The incident at TMI does not give us data as a failure point, because the system did perform its intended function. However, it was a precursor to possible failure and this suggests that we will have to go back and reexamine the RSS predicted failure likelihood for this system to see if changes are needed.

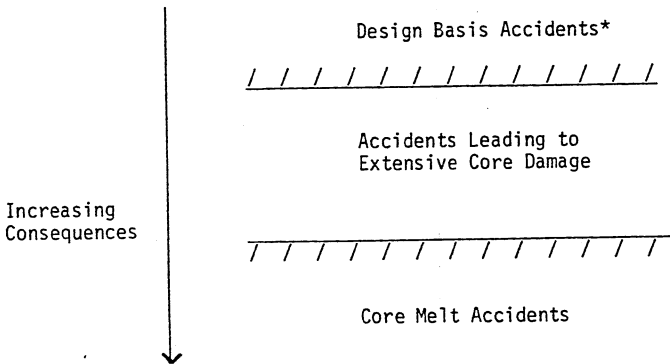
I should also note here that we are now using the RSS techniques to review the auxiliary feedwater systems of all PWR reactors to determine if any upgrading will be needed. It is my belief that the safety engineering insights and techniques developed in the RSS can be used effectively to study the TMI accident to help determine improvements that may be needed in the safety of nuclear power plants. Such an approach is consistent with the recommendations of the Risk Assessment Review Group Report* and with the policies enunciated by our Commission.

* "Risk Assessment Review Group Report" to the U.S. Nuclear Regulatory Commission (NUREG/CR-0400), commonly called the "Lewis Report" after its Chairman, Professor Harold W. Lewis, University of California, Santa Barbara.

RESEARCH NEEDS

The TMI accident has also indicated areas requiring additional safety research information. While some of these requirements can be accommodated by reprogramming and reorientation of ongoing efforts, we believe there will be a significant amount of new work that will require resources over and above those contained in our FY 1980 budget request to the Congress. Therefore, we are currently preparing a proposed FY 1980 supplemental budget request for review by the Commission. While I can indicate now the areas in which I believe research will be needed, I cannot go into great detail because we are still developing this information.

In general, the recent accident at the Three Mile Island Nuclear Plant can be thought of as emphasizing the need for additional safety research information in the area portrayed schematically in the figure below:



*Design basis accidents are defined in the first paragraph of Attachment 1.

Design basis accidents (DBA's) have been studied extensively in NRC's licensing process. A prime example of a DBA is the large Loss-of-Coolant Accident (LOCA). These analyses and supporting research are performed to ensure that plant safety equipment (emergency core cooling systems, etc.) have adequately defined safety margins to prevent significant fuel damage in the event of a DBA. While we have known for some time that more attention is required for small LOCA and transient events, the TMI accident clearly calls for much more urgent action than has so far been taken.

Core melt accidents have been studied extensively in the RSS and ongoing research programs are continuing to better define the physical processes involved in molten fuel and plant materials, the release and transport of radionuclides from the reactor fuel and consequences to the public. Such investigations assign failure probabilities to various safety systems whose lack of operation would lead to core melting. Accidents involving extensive core damage without significant fuel melting were not examined extensively in the RSS because they were not thought to have large public health consequences. The primary application of research about fuel melting to date has been in risk assessment studies which address both the probability and consequence of such accidents.

The area which lies in between these two types of accidents has received less emphasis in both our research program and the licensing process. Such accidents, similar to TMI, can occur as a result of partial failure

of various systems and may lead to extensive core damage, even without fuel melting. I use the term partial failure here to describe two situations at TMI. The first is the fact that a small LOCA occurred when the relief valve opened and failed to reseal. This was followed by the repeated closing and reopening of the block valve to the relief valve, thus, causing a series of intermittent small LOCA's. Also, I refer to the repeated turning on and off of the emergency core cooling system, as opposed to its either complete operability or complete failure.

So far my examination of the TMI accident suggests that research is needed both to reduce the likelihood of events of this type and to obtain a better physical understanding of them. As I said earlier, additional resources will be needed to accomplish this work. The following topics need urgent attention:

A. Transient and Small LOCA Events

Ongoing research efforts must be accelerated to obtain engineering data of behavior of the fuel, the release of fission products from the fuel, and the thermal hydraulic behavior of the core and primary coolant system during transient and small LOCA events. These data are required to accelerate development and testing of analytical models and computer codes needed to give more precise predictions of actual system performance.

More specifically, current nonnuclear test facilities should be modified to obtain engineering data on the heat transfer and coolant flow conditions in the core and reactor primary system for both PWR and BWR transients and small LOCA's. Investigation of the cooling and behavior of fuel under natural circulation and transient conditions where the core may be uncovered would also be performed. Small LOCA tests in the Loss-of-Fluid Test (LOFT) reactor should be accelerated to obtain data with a nuclear core and at larger scale than most of the nonnuclear tests.

Investigations of the behavior of severely damaged fuel which may result from certain transient and small LOCA events should also be conducted. Flow tests of fuel assemblies which have been allowed to boil dry should be performed to study coolability of damaged cores. Tests should also be conducted to determine the rate and nature of radioactive fission product release from damaged fuel, as well as the transport of these fission products in the reactor primary system and subsequent release to the reactor containment.

The development of advanced computer codes to predict more precisely the thermal hydraulic behavior of the core and primary coolant system under transient conditions should be accelerated. These analytical codes, known as "best estimate" codes, are designed to predict with greater precision actual system performance under various transient and accident conditions, as contrasted to the "evaluation model" codes used in the licensing process which contain significant conservative assumptions in order to put an upper bound on predictions of

accident response. The data obtained from the system engineering tests and fuel behavior experiments will be used to upgrade the analytical models and test the prediction capability of the codes. These analytical codes can then be used to analyze a variety of transient and small LOCA events under various failure conditions in order to investigate aspects of plant system design and safety system operation which may require further regulatory attention.

B. Enhanced Operator Capability

The accident at Three Mile Island has also demonstrated the urgent need for system improvements to enhance in-plant accident responses. This area of research need was given high priority and addressed in some detail in the NRC's "Plan for Research to Improve the Safety of Light-Water Nuclear Power Plants" (NUREG-0438), submitted to the Congress in April 1978. This work, which needs to be accelerated, includes improved data display and diagnostic systems to assist the plant operator under accident conditions, additional in-vessel and plant instrumentation which will operate reliably under such conditions, enhanced data transmission capabilities to obtain outside assistance during emergencies, system interlocks to preclude plant operation unless all safety systems are in an operable condition, and development of improved requirements for operator training simulators.

Research should be performed to define requirements for data display and diagnostic systems to better assist the operator under accident

conditions. These display and diagnostic systems should also include the capability for outside organizations to provide assistance and advice to the plant under accident conditions. Studies should be performed to define the necessary data transmission and communication requirements for this purpose.

Improvements are needed in instrumentation to measure plant conditions such as valve position indicators and reactor vessel water level. Studies should be performed to define all instruments needed to assist plant operators in the diagnosis of accident conditions, and tests should be conducted to evaluate and improve reliability of such instrumentation under long term accident environments.

Requirements should also be developed to improve the use of simulators in studying operator response to accident situations and for related training. Control room and plant protection system design requirements should also be studied to define improvements which will enhance accident response and reduce the likelihood that a plant can be operated when safety systems are not all operational. System interlocks which would preclude plant operation under certain conditions should be further defined; such as, unavailability of the auxiliary feedwater system.

C. Plant Response Under Accident Conditions

Research is required to explore more fully the response of plant safety systems and components during accident conditions in order

to understand better the physical processes that can occur so as to help preclude further system failures. Efforts in this area include a detailed understanding of the primary coolant chemistry following fuel failure, hydrogen evolution and behavior in the primary system and containment, and behavior of safety components of the plant, i.e., reactor vessel pumps, valves, etc, under prolonged accident environments.

Experiments should be performed to develop data and analytical methods to characterize the complex chemical nature of the primary coolant after a transient in which some fuel has failed. This work would lead to development of computer codes to describe the coolant chemistry following various accidents, and to the development of improved sampling methods to determine the amount of failed fuel from primary coolant analysis.

Experimental and analytical research should be conducted to describe the formation and behavior of hydrogen in the primary system in accidents which involve significant fuel failure. Research should also be performed to study and predict reliably the mixing of such gases with the containment atmosphere. Methods for reducing the hydrogen gas in the primary system and in containment after an accident should be investigated to reduce the probability of explosion or fire.

Testing should be performed to investigate the integrity of the reactor vessel under thermal shock conditions (cold water on hot vessel) at higher pressures representative of transient and small LOCA events to determine potential for vessel failure. Previous tests of this nature were performed at lower pressures more representative of large LOCA events. Requirements should also be developed for testing of critical plant equipment, pumps, valves, etc., to determine reliability of operation under severe accident environments.

D. Post Mortem Examination and Plant Recovery

It is apparent that significant post mortem examination of the TMI core, plant components and the containment will be very useful in obtaining necessary information on fuel behavior, fission product transport and plateout and component operability under prolonged accident environments. These examinations will also be necessary to help define plant recovery requirements and risks.

The TMI core must be removed from the reactor vessel in a manner such that important configuration information is not lost. The core should then be shipped to appropriate hot cell facilities where it can be examined and analyzed extensively. These studies will provide significant data on coolability of damaged cores, fuel/clad/coolant interactions, and fuel chemistry under severe heat-up conditions.

Examination of the status of the containment building and plant safety components will yield important data on radioactive fission product transport and plateout and provide information on the operability

of safety equipment under prolonged accident conditions. This information will be required to establish improved environmental requirements and criteria for requalification of safety equipment necessary for plant recovery. It is expected that these investigations will also lead to development of improved equipment qualification methodology spanning a range of postulated accidents.

Conclusion

I hope that the views I have expressed here today regarding the safety design philosophy for nuclear power plants and the Three Mile Island accident, including the lessons to be learned from TMI as they relate to our research needs, will be of value to the Committee in its considerations of these important issues. I believe significant regulatory actions are already underway to reduce the likelihood of such incidents significantly. For the longer term, I am sure that further improvements will also be effected. The research areas I have mentioned above should be started soon to provide the needed information.

Loss of Coolant Accident (LOCA)

In evaluating the safety of nuclear power plants in NRC's licensing process, a series of design basis accidents have been selected. A design basis accident is used to specify sets of conditions which engineered safety systems are designed to mitigate in the interest of protecting the health and safety of the public. The most intricate design basis accident is the loss of coolant accident, called a LOCA which is described in the following discussion.

A LOCA is postulated to occur as a result of a break in one of the pipes that comprise the primary coolant system of a reactor.* As a result of the break, loss of cooling capability for the nuclear core would occur and a rise in temperature of the fuel and its cladding could result. Since cooling the fuel and its cladding would be necessary to prevent the release of radioactive fission products, reactors are provided with emergency core cooling systems to keep the fuel covered with water and cooled. A major part of our research effort is devoted to defining the safety margin of emergency core cooling systems with greater precision than is now available.

Figures 1, 2, and 3 illustrate a pressurized water reactor and its associated emergency core cooling system. Figure 1 is a very simplified view of the primary coolant system and the associated steam generating equipment. This shows the reactor core, in its vessel, and the circulation

*More generally, any essentially permanent opening in the primary coolant system that can result in significant loss of water inventory can be termed a LOCA.

of primary coolant system water through the core, out to the steam generator, and back through the pump to the reactor vessel. The very hot water pumped into the steam generator heats other water in a secondary circuit to make steam, which then drives a turbine and a generator to produce electricity. Figure 2 shows how the single reactor core and vessel can be used with up to four cooling loops, each with a pump and a steam generator.

Figure 3 shows how the emergency core cooling system connects to the primary coolant system. The ECCS consists of accumulators, which are large vessels containing water under pressure, and low pressure and high pressure injection pumps shown schematically by the pumps in the figure.

If a pipe were to break, as is indicated in the figure, the primary system water would be expelled as a result of its high pressure and temperature. Signals resulting from the loss of pressure in the primary coolant system would initiate operation of the ECC systems. The efficacy of emergency core cooling performance is predicted by calculating the temperature of the hottest part of the fuel cladding in the reactor core to ensure that it does not exceed NRC's safety requirements. -

Figure 1

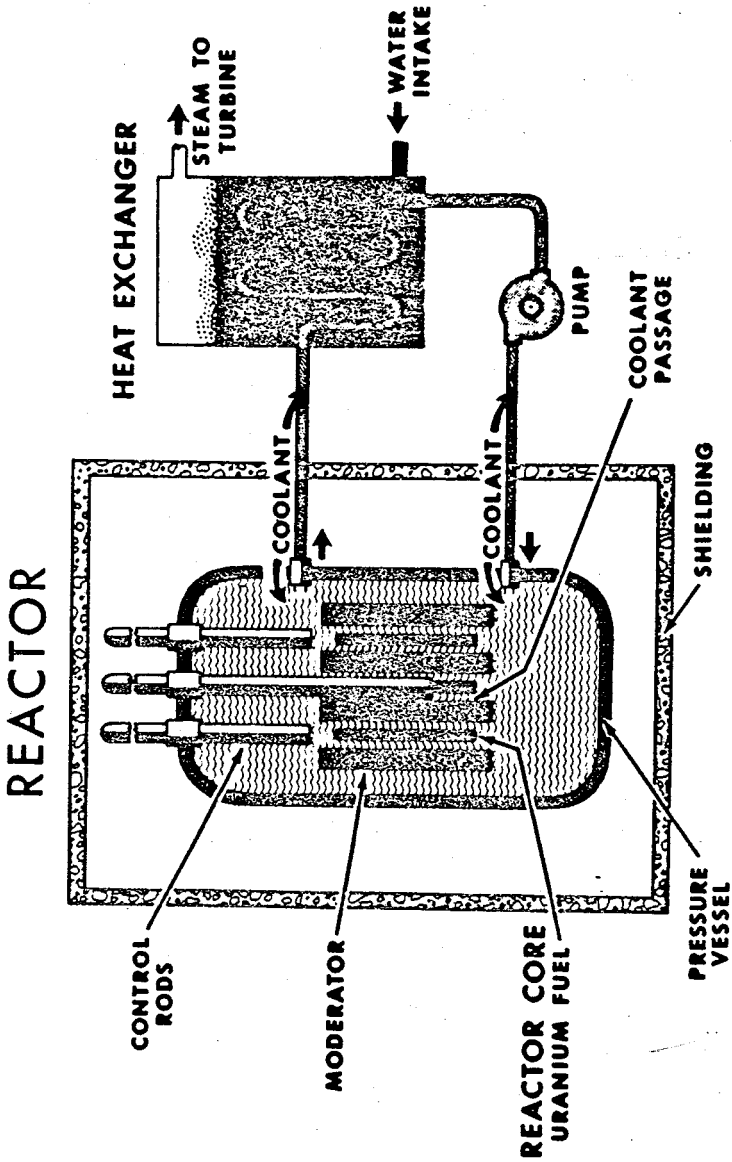
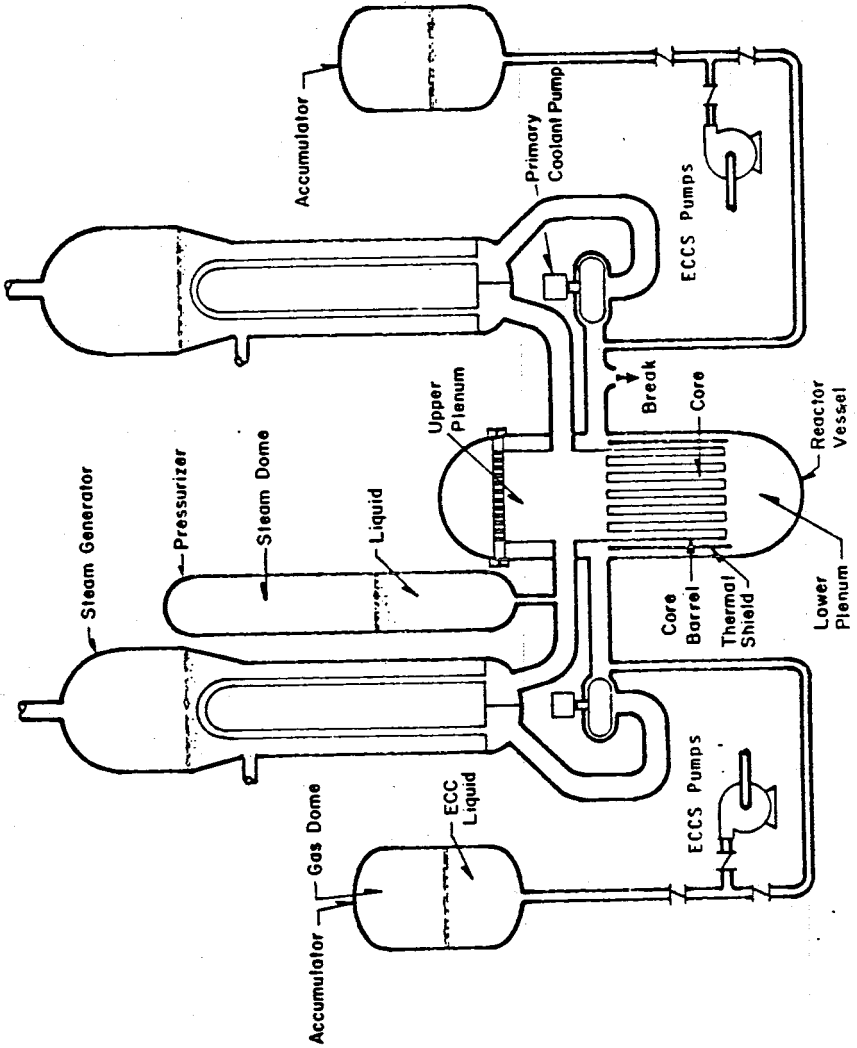


Figure 3



Mr. McCORMACK. Thank you, Mr. Levine.

I have a number of questions which I shall save until after Dr. Lewis. By the way, I should mention, Dr. Lewis is a physicist from—where is your home base, Dr. Lewis?

Dr. LEWIS. Santa Barbara.

Mr. McCORMACK. You are very welcome.

Please proceed with your testimony as you wish, Dr. Lewis.

Dr. LEWIS. Very good; thank you, Mr. Chairman. I am of course pleased to be here. You have my written testimony.

Mr. McCORMACK. Yes.

Without objection, your written testimony will be inserted in the record at this point, and you may proceed as you wish, Dr. Lewis.

STATEMENT OF DR. HAROLD W. LEWIS, PROFESSOR OF PHYSICS, UNIVERSITY OF CALIFORNIA

Dr. LEWIS. Very good. I will forego then reading it to you, because that would waste all our time.

What I do want to say though is that I have to make my position clear. I did chair the American Physical Society Light-Water Reactor Safety Study Group, which resulted in a unanimous report—and therefore I can speak for that group—and the Risk Assessment Review Group which reviewed WASH-1400, which on these matters resulted in a unanimous report, so I think I can speak for that group.

I am also, as of 2 weeks ago, a member obviously of the Advisory Committee on Reactor Safeguards, and I can obviously not speak for that group. So I will try to make clear when I am speaking for myself and when I am trying to speak for one or the other of the groups I have been involved with. I have to put that on the record.

I would like to go through a few of the things you asked me to discuss, rather specifically the problems that our review group found with WASH-1400, the Rasmussen report, and how they are relevant to the question of reactor safety and what they indicate for us. I think I would, especially in view of your introductory comments, like to go through a few of these things, and reinforce some of the things that you have said.

The Rasmussen report, as we all know, was a serious effort to quantify rationally the probability and consequences of a nuclear accident. As soon as it was reported out, it received a great deal of criticism, which was a fairly intimate mixture of rational criticism and irrational criticism, with the result that the entire system became very defensive about the report, and ended up in my personal view defending things that were indefensible along with those that were defensible, and it may be—and we said this in our report—asking too much of people to distinguish among the slings and arrows those which have poison on them and those which are good, clean sharp points. But the group involved did find a certain amount of difficulty doing that.

We studied the report on commission from the NRC for about a year, heard testimony extensively, and ended up saying essentially the following: That the report is very hard to read. I think that is not a great discovery for most people. Everyone knows it is a very hard report to read and to follow in some detail.

On the other hand, it was a major forward step in making the study of the safety of nuclear powerplants rational. It was a serious, responsible, and honest effort—and we said this—to quantify the probability and the consequences of an accident. Where it fell short, and there were plenty of places that it fell short, these were a consequence of the fact that it was a very difficult job that was undertaken.

More specifically, the report used a kind of methodology for the study of nuclear safety, the so-called fault-tree event-tree methodology, which had come under attack from some critics as being wanting in itself. We found that criticism to be without merit, that is to say, we found that the fault-tree event-tree methodology, which is essentially the application of logical procedures to the analysis of nuclear accidents, is a completely solid procedure.

Solid procedures can sometimes be implemented imperfectly, but it is important to distinguish between the quality of the screwdriver and the effectiveness of the carpenter, and we tried to do this.

I am making this point fairly carefully, because one of the important, in my view, recommendations that we made was that this kind of methodology be much more extensively used within the NRC for the orientation of the safety research program, which is under Mr. Levine, and in the regulatory process. That is to say, we said that it is much better to base the things that you do on what knowledge you have than it is to base it on judgment or knowledge derived other than by careful and responsible analysis.

It is an important point, and I would like to keep coming back to it. On the specific implementation in WASH-1400, we went through it, and we did find a very large number of things which were not done as well as we would have liked them to be done. One always asks, in this highly charged and passionate subject, whether errors are made—first, one always asks whether they are made on purpose, and we answered that by saying no.

Then one asks whether such errors as are made have the consequence of exaggerating or minimizing the likelihood of a reactor accident, that is, in the jargon of the trade, are they conservative or nonconservative? We found that there were a fair number of conservative things, overly conservative things, and I can name a few of them. I will come back to one important one. And there were a fair number of nonconservative ones, that is, things in which the probability of an accident was understated.

There were so many things on both sides of the fence that our group ended up saying that we do not believe that the probabilities stated in WASH-1400 are as credible as they are alleged to be, that is to say, that the error bounds are greater than was stated in the report. But we also were not able to say, and did not say, that the probabilities calculated in the report are either high or low, that is, we did not say the group came out with either an understated or an overstated estimate of the probability of a reactor accident.

However, we said that the estimates weren't as good as plus or minus a factor of five, which is what was stated in the report, weren't that good, because we found many things with which we found fault.

Thus, we essentially commended the methodology. We said it is a good way to do things. It is better to analyze safety through analysis where you can, but that perhaps it was too big a bite that was taken at the time of the Rasmussen report.

We urged the NRC to move in the direction of using this kind of analysis on systems which were sufficiently small so that the data base was available, the statistical techniques were available, the ability to describe the system under consideration was there, so that you could do the job in a credible and effective way, that they should be doing that much more than they had been doing so in the past.

One example, for example, of that sort of thing is that the Rasmussen report—let me make one other comment. This is a personal comment. When the NRC received our report, there followed 4 months of Commission meetings about what to do with it. It was too late to reverse time, so they couldn't just throw it away, and after 4 months the NRC essentially accepted all the recommendations of our report and directed the staff to move in the direction of using this kind of methodology much more than they had in the past. This was of course accompanied by a press release which was misunderstood.

Well, many things were misunderstood. It is in the nature of man that things are misunderstood. But they also asked the staff to report back to the commission whether in fact the Rasmussen report had played a role in any of the licensing and regulatory decisions that had been made in the few years it had been around, and the staff reported back that, with the exception of a few rather minor instances, no, it had not been used, and everyone was very pleased by that, and I have always felt that that was the wrong answer, that in fact in the years between the time the Rasmussen report was given to the NRC and the time in which we found some substantial problems in it, it was the best thing available, and should have been used much more extensively than it was. That is to say, risk assessment methodology is a solid discipline and should be used as much as possible to guide the regulation and licensing of reactors.

One specific, which I have pulled out of our report from last September, and I must read this one paragraph to you from the record, was that we noticed that in WASH-1400, whatever you think of it, there was a listing of many of the credible accidents in a plant, and an ordering, that is to say, one could identify in WASH-1400 with less credibility than had been thought before, but still with some credibility, what the most likely accidents were, and we found a problem with the fact that NRC had not been moving in the direction of studying and emphasizing those things which WASH-1400 showed to be most threatening to a nuclear power-plant.

We have a paragraph:

The achievements of WASH-1400 in identifying the relative importance of various accident classes have been inadequately reflected in NRC's policies. For example, WASH-1400 concluded that transients, small LOCA, and human errors are important contributors to overall risk, yet their study is not adequately reflected in the priorities of either research or regulatory groups.

Now those are the three things that were relevant to Three Mile Island, so there is an obvious lesson which I needn't belabor. In any

case, we did recommend using the methodology, pushing it much harder. We found specific fault with WASH-1400, and I think that is really all I need to say. Our detailed conclusions are in our report, and I am happy to answer any questions you may have.
[The prepared statement of H. W. Lewis follows:]

TESTIMONY OF H. W. LEWIS
BEFORE THE SUBCOMMITTEE ON ENERGY RESEARCH
AND PRODUCTION OF THE COMMITTEE ON SCIENCE AND TECHNOLOGY
OF THE U. S. HOUSE OF REPRESENTATIVES
MAY 22, 1979

I appreciate the opportunity to appear before you today to discuss a number of issues of risk assessment, and of technology developments to enhance the safety of nuclear operating systems. As you know, I was Chairman of the American Physical Society Light-Water Reactor Safety study group, and also of the Nuclear Regulatory Commission's Risk Assessment Review Group, and have only two weeks ago become a member of the Advisory Committee on Reactor Safeguards. The two former studies resulted in unanimous reports on all the issues to be discussed here, so that I will do my best to speak for the Groups where it is appropriate. In addition, I would like to express a number of my personal views, and will try to distinguish the two roles as carefully as I can. Clearly, I do not speak for the Advisory Committee on Reactor Safeguards.

You have asked, in your letter of May 11 that I outline which elements of the Rasmussen report our Review Group judged invalid, and the degree to which the report is still useful as a basis for decisions by NRC. I would like to somewhat broaden the issue, since the charter of the Review Group was to study not only the Rasmussen report itself, but also the general subject of risk assessment methodology, and many of our recommendations dealt with the distinction between the two. I will try to make all that clear.

Probabilistic risk assessment, as epitomized by WASH-1400, the Rasmussen report, is an effort to make quantitative the risk of an accident (not just in reactors) and the consequences thereof. To do so it is necessary, at the very outset, to construct a detailed model of the operating system, which

must be complete and accurate. Accident probabilities may differ vastly according to the precise alignment of valves and switches, and generalizations are rarely sufficient for credible accident analysis. Having modeled the plant, there are then a number of techniques for tracing accident paths through the system, all of which are essentially equivalent to the particular form of fault tree/event tree analysis used in WASH-1400. If one has sufficient data to determine, for example, the probability that a given valve will be open when it should be closed, one can then compute the probability of any particular accident sequence, leading to an estimate that it will lead to failure of the entire system. Then, similarly, one can compute the consequences of such an accident, and this is the method used in WASH-1400.

The Review Group asked first whether this was a logically sound technique, and answered in the affirmative. It is extremely difficult, and fraught with complexities I will mention later, but we solidly supported both the methodology and the objective of making the study of reactor risk as quantitative and rational as possible. Nonetheless, we found faults in the implementation of the methodology in WASH-1400, which are discussed in some detail in our report. Among them are the fundamental difficulties involved in quantifying common cause failures -- failures in which presumably independent systems are compromised by an event which affects them all, (e.g. an earthquake), a quite inadequate data base for a number of the things which needed to be calculated, inadequate, and sometimes wrong, statistical techniques in a number of important places, the basic difficulty in quantifying human behavior, etc.

Therefore, though supporting the methodology, we found a sufficient number of problems with the implementation of the methodology in that particular study to feel that the error bounds on the accident probabilities given in WASH-1400 were substantially understated. It is important to say that this does not mean that we believe that the accident probabilities are either high or low, but only that they are substantially less certain than was stated in that report.

This is such an important point that it is worth spelling it out in some detail. We found a number of items in WASH-1400 which tended to exaggerate the probability of an accident (i.e., were conservative), and a number which tended to understate the probability of an accident (i.e., were non-conservative). Among the latter were the treatment of common cause failures, mentioned above, the treatment of ATWS (anticipated transients without scram) and the handling of human accident initiation. Among the conservative treatments were the pervasive regulatory bias in the group, drawn as it was from the regulatory community, which caused them to always err on the side of conservatism when in doubt, complete omission of constructive and adaptive human response during the course of an accident, etc. It is because there were so many things on both sides that we were unable to judge whether the probabilities in WASH-1400 were high or low, but able to agree unanimously that they were substantially less precise than had been stated in the report.

On the other hand, the effort to quantify risk through the detailed analysis of the failure modes of a plant is far more likely to provide rational guidance to safety enhancement than is guesswork. For that reason, we strongly

supported the application of this kind of risk assessment methodology in the regulation and enforcement areas, under conditions in which the data base and statistical techniques are up to the job, that is, on subsystems and generic issues sufficiently limited to allow one to do the job well. Indeed, we said that these techniques should be among the principal methods used to resolve the generic safety issues which afflict the nuclear enterprise.

I am emphasizing these distinctions because our Review Group strongly supported the enhanced use of the methodology in the regulatory process, while at the same time coming down rather hard on the specific implementation in WASH-1400. It seems to me obvious that, where one has an opportunity to understand the relative importance of different accident modes in the plant, and even, to some extent, the absolute probabilities, it is far better to distribute one's resources accordingly than to rely upon engineering judgment, however competent. Though the latter is extremely important, and represents in some sense the distillation of accumulated experience, it cannot prevail in reliability over competent analysis. We therefore urged, as others have been urging for years, that the NRC move expeditiously into a mode in which probabilistic risk assessment plays an important role in determining the priorities of its regulatory and research efforts. I would like to quote verbatim one of the findings from our report, whose relevance this month should be obvious.

"The achievements of WASH-1400 in identifying the relative importance of various accident classes have been inadequately reflected in NRC's policies. For example, WASH-1400 concluded that transients, small LOCA, and human errors are important contributors to overall risk, yet their study is not adequately reflected in the priorities of either research or regulatory groups."

This paragraph speaks for itself in the aftermath of Three Mile Island. I believe that the effective use of risk assessment methodology in characterizing and dealing with the risks in reactors can go a long way toward making them safer, as well as in helping to assess their safety for public policy purposes. For this to happen, the NRC research program must be more responsive to the risks as determined by sober analysis, and less responsive to the risks as conceived in other ways. Even the progress already made in rationally characterizing and understanding risk has been very slow to penetrate the regulatory structure at NRC, and our report recommended that "NRC should encourage closer coordination among the research and probabilistic analysis staff and the licensing and regulatory staff, in order to promote the effective use of these techniques." Despite the statement of the Nuclear Regulatory Commission last January that it was accepting all our recommendations, and its instructions to the staff to move in this direction, I have yet to see much progress. This is not to demean in any way the technical quality of the NRC operation, but only to say that the conservatism which

is entirely appropriate in the regulatory body does not lend itself easily to the absorption of new guidance.

Finally, I am both pleased and sorry that you have not asked me to tell you what lessons I believe Three Mile Island has taught us about all these matters. I am pleased because you have saved me some work, and sorry because I believe that there is so much that we can learn from experience in general, and from this experience in particular. Perhaps someone will rise to the bait and ask me a question.

Mr. McCORMACK. Thank you, Dr. Lewis. I want to take this opportunity to congratulate you and all the members of the panel that worked on the review. I do not purport to be the wisest person nor the most knowledgeable person on this subject, but I think that your review was an excellent one, and I want to congratulate you on it. I regret that it was misinterpreted by the press. I regret that NRC's press release regarding its action on it was so ineptly written, I think that your work made a very considerable contribution. I recall previous meetings, public hearings where you and Dr. Rasmussen appeared together, he agreed with that statement, and in the true character of a professional scientist, accepted the criticisms, at least a substantial portion of the criticism that you made of his report, and agreed with them. I want to congratulate you also on the professional manner with which you evaluated the report.

I think that in the days to come, the Rasmussen report and your analysis of it will both contribute significantly to the better understanding and better management of our nuclear safety programs.

Dr. LEWIS. Thank you, Mr. Chairman. You will make me blush, but it is true that Norm Rasmussen has accepted essentially all the recommendations of our report also, and I give him a great deal of credit for behaving like a gentleman and scholar through this whole thing.

Mr. McCORMACK. Especially a scholar, and without detracting from the gentleman, but especially a scholar.

Dr. LEWIS. Yes.

Mr. McCORMACK. I would like to ask you a question now in that context. You said the factor of plus or minus 5 which they used in their error bounds was too narrow.

Dr. LEWIS. Right.

Mr. McCORMACK. Do you feel there is a number that you could put on the error bounds that would be realistic?

Dr. LEWIS. No, I do not, and we were very careful not to do that. We said substantially understated or greatly understated, and people have tried to pin us down, and particularly Norm Rasmussen I think is willing to go another factor of 2 or 3, and we have had conversations that were almost like bartering sessions. If I would go for a factor of 5 perhaps we could compromise on a factor of 4 extra over the 5.

The reason we cannot do that is that, in other words, to provide a credible error bound, we would have to do the report over again.

We would have to do it responsibly and even better than the Rasmussen group did. In a sense the reason they could not set an error bound that stood the test of time was that they were biting off a very, very difficult job. There are intangibles. There are things we do not know.

We really did not know how to quantify human errors. My view of the great conservatism in the report is that we do not know how to quantify constructive human intervention after an accident begins. These are very difficult, and in order to set a credible bound, one would have to do all those things better than the Rasmussen group did. We did not do that.

Mr. McCORMACK. Do you have any feeling for the general impression that the casual nonscientific, nonanalytical observer would receive from reading in the Rasmussen report that the potential for an individual public citizen being killed from a nuclear accident is extremely small, whether or not we try to quantify it numerically?

Dr. LEWIS. Is your question whether I agree that the probability of being killed is small?

Mr. McCORMACK. I do not want to put you in the position of saying "agree," but do you believe, based on your study, that the potential threat of death from a nuclear accident to public citizens is extremely small?

Dr. LEWIS. Yes. I am speaking for myself now, just me. Yes, I do, and in fact I have said many times that if I were to be asked personally, not as chairman of the review group, whether I think that the probability of an accident stated in the Rasmussen report is high or low, the thing I carefully avoided saying before, I feel that the probability of an accident stated in that is high, that is to say, that the plants are actually safer than is stated in the Rasmussen report. I said that before Three Mile Island and I continue to say it.

The reason I say it is that as the people who listen to me know, to their misery, I always make aviation analogies in these things. And the Rasmussen report, in effect, if it were translated into the aviation case, would be like studying the safety of airplanes while leaving out the fact that there is a pilot there who does not want to get killed either, and the fact that constructive human intervention during the course of an accident was omitted is to me a very important conservatism in the report.

It is very difficult to quantify, but reactor accidents lend themselves more easily to constructive intervention than do aircraft accidents, because they happen more slowly. Most of them happen more slowly, the ones that are most threatening happen more slowly, so I do believe that it exaggerates the probability of an accident.

Mr. McCORMACK. One final question. Do you feel that the Three Mile Island accident and the subsequent sequence of events, fit reasonably well into the Rasmussen evaluation of the fault-tree risk analysis?

Dr. LEWIS. Yes; they fit into it to some extent—that is, everyone has noticed, that the probability of leaving the two block valves on the emergency feed water system inadvertently closed was contained in the report. It was calculated, I believe, in an inexcusably

poor way, but it was still in the report, so that up to the point at which the hydrogen bubble formed in the pressure vessel, it was not an unusual sequence of events.

By then one was in the position to do a diagnosis and work through what finally happened. I believe it was done reasonably well in the report.

Mr. McCORMACK. Thank you.

Mr. Levine, I have one question which I hope will not be misconstrued. One looks at the Three Mile Island accident in its entirety, the fact that it was a serious accident, that it was extremely unfortunate, and yet one looks at all that we have learned from it.

We have learned, for instance, that under the nearly noncredible conditions that existed with respect to the exposure of the fuel, the uncovering of the fuel, we had no cesium release to the coolant water. In short, what we had was a massive LOCA experiment, unintentional experiment. Do you feel that this qualifies as a test for a fuel core that has been lacking because we obviously did not want to do it? Does it respond to the criticism of the LOFT test that they are not big enough? Can we draw experience from this accident and draw knowledge from this accident that will give us a better understanding and essentially say, well, this is for all practical purposes an unintentional LOCA experiment?

Mr. LEVINE. I think the answer is partly yes and partly no, and certainly not yet. First of all we are going to have to get the core out of there to understand more precisely than we can now estimate, what happened to it, how extensively it was damaged, and then try to better predict what the temperature-time history of that fuel was.

Second, I think the idea of trying to analyze an accident in which the auxiliary feed water was turned off and then later turned on, and the emergency core cooling system was turned off and on at random, and the relief valve block valve was opened and closed, giving it sort of an intermittent LOCA, is a kind of sequence that is very difficult to analyze.

For myself, at this point I can say that I think, considering what happened at that plant, I am surprised that there was not more damage than we have seen, and I think in that sense, one can say we will have learned a great deal about the ability of these cores to withstand severe conditions.

On the other hand, we are learning a great deal from our LOFT program. We have now conducted two nuclear tests, one from two-thirds of the power density of a commercial reactor, and just a few weeks ago, one from the full power density of a commercial reactor. We find the peak clad temperatures quite low, and we find our ability to predict what happens to be quite good. Some more refinements are needed, but I think we are making great strides in this area.

Furthermore, I think we are going to have to modify our LOFT experiments to more urgently look, at small LOCA, as I mentioned in my testimony, as well as transients, too.

Mr. McCORMACK. One final question. You may not have an answer at all to this. I have been continually disturbed by the calculations on the amount of zirconium that was presumably consumed. It seems to me utterly inconsistent to talk about as much

as one-third of the zirconium consumed, based on the amount of hydrogen that was presumed to be present, and to assume that this came from the top half of the fuel, to assume that there would be a hot spot, shall we say halfway between the surface of the water and the top of the fuel, where more of the zirconium would be reacting. All this happens, and we have one-sixth of the total zirconium consumed, and yet no cesium is released to the cooling water. That strikes me as being very strange, and I wonder if you care to comment on it.

Mr. LEVINE. I can only comment on the basis of generalizations at the moment. We think that there was almost no fuel melting in the core, and that you really will not get very much cesium released unless you melt the fuel.

On the other hand, the core did reach high enough temperatures to bake out iodine and the noble gases, and there may have been an eutectic formed between the oxide and the cladding, which would in fact have released more than you would get just through the temperature alone.

Mr. McCORMACK. More what?

Mr. LEVINE. More of the iodine.

Mr. McCORMACK. And gases?

Mr. LEVINE. Yes.

Mr. McCORMACK. Are you suggesting—well, I guess my question is when I see no cesium at all, no significant measurable cesium in the cooling water, I am assuming that there was no contact between the cooling water and the fuel itself.

Mr. LEVINE. That may be, but there surely was a large metal water reaction in some parts of that core.

Mr. McCORMACK. Yes.

Mr. LEVINE. And it is easy to speculate that there was cladding damage to the point where some fuel should have been exposed.

Mr. McCORMACK. Should have been, but that is the inconsistency that shows up, and I am raising that point now.

Mr. LEVINE. I think in my mind that is still an open area. We have some differences of view among our experts who have been studying this very carefully, and by the way, the metal water reaction amount was not based just on the hydrogen present. It was based on attempts to reconstruct the time-temperature history of the core.

Mr. McCORMACK. I see. Thank you.

Mr. Goldwater.

Mr. GOLDWATER. Dr. Lewis, discussing the WASH-1400 report with Mr. McCormack, you implied that an update should be made on that report. Is that an accurate interpretation?

Dr. LEWIS. No; I do not think so. On the specific question of whether WASH-1400 should be updated or redone, I do not think it would be a good idea. There are several reasons. Of course we could do a little bit better with the hindsight we have had, but I am not so sure that we could do enough better to justify doing it. The sense of our review group report was that one should break out the methodology and use it on subsystems for which you can do the job well, rather than on the whole system, for which it may not be possible to do the job well.

Mr. GOLDWATER. You implied that there was not enough risk assessment based on transients, small LOCA and human error, incorporated in this study.

Dr. LEWIS. Oh, no, no, quite the opposite. It was in fact in WASH-1400. One of the consequences of WASH-1400 was that transients, small LOCA, and human error do play an important role in the generation of nuclear accidents. The place where it is inadequately represented is in the NRC programs which ought to have been more responsive to WASH-1400 in my view, well, in our group's view, than in fact they were. NRC is a slow-moving organization. Perhaps it is proper for a regulatory organization to be slow-moving, but it would be nice to have some of the wisdom which was produced by WASH-1400 including the importance of small LOCA transients, and human error find its way into the NRC research and regulatory structure. It is in WASH-1400.

Mr. GOLDWATER. So you feel that the two reports, your review and the WASH-1400, have sufficient standing separately and they don't need to be incorporated?

Mr. LEWIS. Our report was a fairly strong critique of WASH-1400. I have emphasized the positive things we said today, but in fact, we were fairly hard on the report in terms of statistics, data base, scrutability, and such matters. So that we found a great deal wrong with it.

When I say that I don't believe it would be worthwhile to do it again, it is just I am thinking of the millions of dollars, man-years, expertise, and effort involved. I think if that same amount of effort and resources were to go into applying the methodology where you can do it well—that is, on subsystems—that would be a better expenditure of our time.

Mr. GOLDWATER. What do you believe are the basic lessons that we should or will be learning from the Three Mile Island accident?

Mr. LEWIS. Well, I have views on that. Basically, I think I can do this very quickly. I think many people have noticed that there are a wide variety of accidents and that in this particular event there was a surprise—the formation of the gas bubble in the pressure vessel was a surprise.

The thing that concerns me about the lessons people are drawing from Three Mile Island is that they tend to be rather specific to the particular sequence that occurred at Three Mile Island; that is to say, the familiar analogy, a horse has escaped from this barn and we are double bolting that particular door.

We tend to be fairly narrow in responding to the specific thing that has happened. I think any future accidents—and there will be accidents—will also contain surprises. The main lesson I learn, again drawn in part from the aviation analogy, from both Three Mile Island and from Browns Ferry, which was the worst thing up to now, is that in the end it takes constructive human intervention to modify the course of an accident. That happened in both cases, and it will happen again.

So I would like the main lesson to be that you provide to the operators the kind of information, training, awareness, and what have you, pay, perhaps, prestige, stewardesses, I don't know, that makes it possible for them to function like airplane pilots, during the course of an accident.

There is plenty of time. I think flexible response is the key to keeping an accident from going far enough down the track to threaten the public health and safety. For me, that is the central lesson.

Mr. GOLDWATER. You are talking about the quality of the person.

Mr. LEWIS. No, the person and the stuff he has available; that is to say, many people have commented on the fact that some of the instrumentation was deficient, the parameter range wasn't large enough to encompass accident conditions, there are no valve indicators on specific things.

Many of my physicist friends have reacted to the accident by saying that there should be an interlock on the two block valves that were inadvertently left closed so they could not both be left closed, there should be indicators on all the valves in the plant.

I don't think that makes any sense, but there should be an analysis of the critical systems in such a way that one provides to the operator the necessary indications to know what to do in the event of an accident.

For example, I don't like to second-guess what the operators at Three Mile Island did because I am aware that it is very, very easy to do things well in retrospect and not so easy to do them in real time.

But there were some deficiencies in correlating readings and correlating indications which would have told them more about what was happening in the plant than they seemed to have absorbed very quickly.

I would like to enhance the capability one way or another by providing the instrumentation and training to make it possible to do that. But I do believe that in the end, people are fairly intelligent creatures and you have time in a reactor accident, and if you make the information available you have a great weapon we should use. It is hard to analyze.

Mr. GOLDWATER. Maybe a parallel toward an automatic pilot on an aircraft is a good analogy. An automatic pilot will fly that airline, and does most of the time. But there is adequate instrumentation to provide the pilot and the engineer with knowledge of what is happening to the aircraft.

Mr. LEWIS. That is correct. A good pilot——

Mr. GOLDWATER. However, when there is a problem with an aircraft, say for instance the plane starts to wiggle its wings or something, the pilot tends to kick the thing off and assume manual control.

That appears to be what happened at Three Mile Island. I have heard people say if they just let the emergency core cooling system alone, that it would have shut down, taken care of itself. But in fact, a human being intervened, much like the pilot on an aircraft overriding or cutting out an automatic pilot.

Now, I am not so sure that is what you are saying, is it?

Mr. LEWIS. I am saying that; that is to say, the other thing that the pilot of an airplane learns is to believe his instruments because it is normal human response when an instrument indicates a malfunction to not believe that it is happening to you.

He learns to believe his instruments. He also learns to correlate his instruments; that is to say, he doesn't fix his attention on a

single instrument. You are right. A good pilot turns off the autopilot when he is in trouble. But he correlates all his instruments, he reads them, and he infers what is happening and does his best to get out of it. It seems to me that that works pretty well.

There is a fairly deep-seated analogy between aviation and nuclear power in my view from which a lot of lessons can be learned—because aviation is an inherently risky thing which has become acceptably safe.

Mr. McCORMACK. Mr. Walker?

Mr. WALKER. Thank you, Mr. Chairman.

Dr. Lewis, you had mentioned in reaction to some questions of the chairman that it was your personal opinion that the chance of death in the general population resulting from a nuclear accident was extremely small.

Can I ask you also what your personal opinion would be of the chances of off-site property damage resulting from a nuclear accident? Would that be significantly higher? Is it also relatively small in terms of some sort of calculated risk?

Mr. LEWIS. You know, to say that something is small or large is not to say anything meaningful, because smallness and largeness are in the eye of the beholder.

What I said in response to the chairman's question I hope is that it is my personal view that the probability of an accident, of a genuine major reactor accident, is lower than is contained in the Rasmussen report. That would carry with it the consequences that the probability of property damage is also lower.

But I base that almost entirely on the experience we have had with the two major accidents, plus a fair amount of carryover from aviation, that one will intervene in an accident and keep it from getting too bad.

Mr. WALKER. That goes to the point I was going to raise. From your standpoint, then, the Rasmussen study exaggerates the probability of an accident?

Mr. LEWIS. That is my personal view.

Mr. WALKER. OK. Now, given that background, we had a group of Nobel Prize winners before the committee here a week or so ago—not before this subcommittee, but before the full committee—they were essentially nuclear advocates.

One of the things that they mentioned, that might be a good idea, from the standpoint of the nuclear industry would be to repeal the Price-Anderson Act. I bring this up to you because it seems to me the kind of research that the Rasmussen study represents, to some extent your study represents, is also something which applies not only to the nuclear industry, but also to public policy decisionmaking.

In large part Price-Anderson and some of these things are built upon that kind of research. So my question to you would be, if we are exaggerating in those studies the foundation on which some of these decisions have been built, would it be reasonable to consider the repeal of Price-Anderson and have the industry assume liability for any accidents that would involve the public?

Mr. LEWIS. I do not claim to be an insurance expert.

Mr. WALKER. I am asking you from the research standpoint. Research is the foundation on which the insurance people are basing their calculations.

Mr. LEWIS. Of course, I know all your Nobel Prize winners were here. I also remember that Edward Teller at one stage in the proposition 15 debates in California used to complain that if he were immortal he could not get life insurance because there would be no data base for determining the premium, and that was his way of putting it. I am not an expert on that.

I would like to see the research directed at the places where there are problems. I would like to see somebody go through all the accident sequences in WASH-1400 and for each one—there are really a finite number—say if this were to happen, do we have the training and instrumentation to know how to keep it from going all the way down to a core melt.

Perhaps if one did that, one might be able to put something quantitative on my admittedly visceral feeling that one has exaggerated the probability of an accident.

Mr. McCORMACK. Will the gentleman yield for one point.

I would like to make one point; that is, as a matter of history, the Price-Anderson Act was enacted long before the Rasmussen report was made.

It was enacted in the 1950's to protect small contractors, not the big vendors, but the small contractors, so that they would not get caught in second party lawsuits, or third party lawsuits.

What it did was require that the utility buy the maximum insurance available in a pool. The later modification of the law, of course, specifies that the industry provide contributions up to a total of \$560 million.

When the Rasmussen report was being done, those persons who were trying to repeal the Price-Anderson law said just wait until Rasmussen comes out, then we will use that to repeal Price-Anderson.

When it came out, reporting as it did, that the possibility of death from a nuclear power accident was very low, then they turned against the Rasmussen report.

I just want to get that little point in so we keep in perspective the fact that in reality the Price-Anderson Act precedes by at least a decade any of these studies, and it was there for a totally different reason than the results brought out.

Mr. WALKER. I thank the gentleman for that clarification. What I was simply trying to get at was the fact that the public policy decisions that we are going to be asked to make in upcoming months are very much based upon the kind of research that Dr. Lewis has provided here and that has been provided earlier by the Rasmussen studies.

I think it is extremely important that some of the people who have had some experience with the research, and have knowledge of it, give us their perspectives. This would let us make those public policy decisions, maybe, exclusive of what is going on within the technological elements of the nuclear industry.

I thank the gentleman.

Mr. McCORMACK. I think the gentleman's point is very well taken and I congratulate him for it.

Mr. WALKER. That is all I have, Mr. Chairman.

Mr. McCORMACK. Mr. Goldwater, do you have anymore questions?

Mr. GOLDWATER. I have one more.

I didn't quite follow, Dr. Lewis, your analogy about the probability of risk or the risk of nuclear accident versus the risk of an aircraft accident. You were making a point to the chairman.

Is there a higher degree of risk of a major aircraft accident than there is, say, for a nuclear powerplant accident? Is that what you were saying?

Mr. LEWIS. I don't remember which specific comment you are referring to. The analogy, as I see it, is that in both cases you have a complex system which is very hard to analyze from the beginning; that is, it is extremely difficult to analyze all possible aircraft accidents from the beginning, too.

So that what we have in the case of aircraft that has made the industry acceptably safe, although there is still some residual risk, is a system by which we have a pilot up front who is well trained in upset conditions, with redundant instrumentation devoted to those conditions and with enough training on good aircraft and simulators so that he can cope constructively with the course of an accident.

We also have a bureaucratic procedure in the best sense of the word, not the worst, by which those few things that do continue to happen are then analyzed to death and the learning from them put back into the system.

Over the years, that has made aviation acceptably safe. I have in other forums been recommending for years that something like an NTSB structure be applied to the nuclear industry.

I might just comment that when this suggestion went over to NRC about 6 months ago, one of their answers was, these people wouldn't have anything to do because there aren't any accidents. Perhaps it wouldn't be the same now.

Mr. McCORMACK. Thank you.

First of all, I want to thank these witnesses, and again thank the witnesses from the earlier panel. The contributions that you have made today, and the specific points that you have made, Mr. Levine, about the need for future research, will be the basis for future legislative action by this committee. We appreciate it.

We appreciate what you have contributed and we appreciate again your contribution, and your perspective, Dr. Lewis.

I want to also thank the members of the French Parliament who sat in today. We offered them a chance to ask questions, but since none of the members themselves actually speak English, we decided to forego the pleasure, especially since it is getting late.

We want to thank them. We know that they will have questions later on. In that regard, I am sure the witnesses will be glad to answer questions in writing, either from us or from the French Embassy.

Tomorrow, starting at 9:30, this committee will meet again, and we will concentrate specifically on what happened at the Three Mile Island accident.

We are going to see, first of all, a demonstration of a nuclear powerplant, which will be here. It has been manufactured by the

University of Florida, and it has a high intensity heater system with cooling systems built in. It is all made of Lucite, so we can actually see standard operating conditions, the way it would be with a partial meltdown, with the emergency core cooling systems functioning and so on. We will actually be able to see it in operation.

We will also hear witnesses from Babcock & Wilcox, the vendors for the Three Mile Island plant, from Mr. Herman Dieckamp, president of General Public Utilities Corp., Mr. Harold Denton, Director of the Office of Nuclear Regulation of NRC, Mr. John Conway, president of the American Nuclear Energy Council, and Hon. William W. Scranton, the Lieutenant Governor of the Commonwealth of Pennsylvania.

We will convene tomorrow at 9:30. We thank you all for your attendance today. We stand adjourned.

[Whereupon, at 12:15 p.m. the subcommittee adjourned, to reconvene at 9:30 a.m., Wednesday, May 23, 1979.]

APPENDIX I
QUESTIONS AND ANSWERS FOR THE RECORD

C-E Power Systems
Combustion Engineering, Inc.
1000 Prospect Hill Road
Windsor, Connecticut 06095

Tel. 203/688-1911
Telex: 9-9297



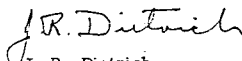
June 22, 1979

Hon. Mike McCormack
Chairman, Subcommittee on
Energy Research and Production
U. S. House of Representatives
Suite 2321 Rayburn House Office Bldg.
Washington, D. C. 20515

Dear Congressman McCormack:

It is a pleasure to submit further information to the Subcommittee on Energy Research and Production in the form of answers to the questions you asked in your recent letter. The answers are appended. I hope you will find them useful.

Sincerely yours,


J. R. Dietrich
Chief Scientist
Nuclear Power Systems

JRD:jd

Enc.

SUBCOMMITTEE ON ENERGY RESEARCH AND PRODUCTION

Answers to questions from the May 22, 1979 Hearings on
Nuclear Power Plant Safety, by Joseph R. Dietrich

In answering questions 1 through 5, I must make it clear that in my testimony on May 22 I was speaking of design reviews and studies, some of which are under way and some of which were merely recommended. The substantive answers to questions 1 through 5 must come from such reviews and studies. My recommendations are, therefore, as to what should be studied. Here I can only give examples of changes that have a potential for enhancing safety. Moreover, as I pointed out in my testimony, any proposed design change of substantial magnitude must be given a very thorough engineering review on a systems basis before it is made, to assure that it does not, while improving safety under one set of circumstances, degrade safety under other circumstances.

Question 1

Discuss the design changes or modifications and the procedural changes that you would recommend to minimize the frequency of occurrence and the speed of development of the operational perturbations mentioned in your testimony.

Answer

This class of improvement would be accomplished primarily by design changes. Some possibilities to be considered might be additional pressurizer volume to simplify the maintenance of primary system water inventory; anticipatory reactor trips (e.g. trip upon loss of normal feedwater flow as well as on low steam generator water level); generous water inventory in the steam generators to increase the time available to restore feedwater flow in the event it is lost; and, possibly, multiple relief valves of smaller size, with graduated pressure settings, to minimize the flow out of the primary system if the transient causing a relief valve to open is a minor one. In the latter case the relief valves would of course have block valves in series to be used in the event that a relief valve failed to close at the proper time.

I am sure that there are many more possibilities, but they must be sought out by examining each transient that might occur and looking for design changes that would decrease its probability or its severity. Most design changes that would fall into this class would be impractical to implement on existing plants; consequently an investigation of these possibilities would have its major application to new, rather than existing, plants.

Answers to Questions - J. R. DietrichQuestion 2

What design changes or procedure changes would you recommend to improve the defense against lesser accidents that you referred to in your testimony?

Answer

This again is a question that can be answered only by extensive study and analysis. For the immediate future my only suggestion is that we give more attention to the lesser accidents in our safety analyses of nuclear plants, and more attention to the possible interactions between the operator and the plant. The initiating events at Three Mile Island would have been classified as constituting a "small" accident in safety studies in the past, yet they were escalated into a major accident. Greater attention to the possible consequences of "small" initiating events should lead to improvements in design and operator education which will greatly reduce the probability of such escalation in the future.

Questions 3, 4, and 5

- 3) Provide details of the improvements in communications and the man-machine interface that you suggested in your testimony.
- 4) Provide details of the means of simplifying the interpretation of instrument readings, together with your recommendations for displaying abnormal readings.
- 5) Discuss and provide recommendations for means of using computers or microprocessors to enhance the power plant operator's ability to recognize abnormalities.

Answer

Questions 3, 4, and 5 apply to closely related subjects, and can best be discussed together. I could respond at great length to these questions because they cover a specific field in which Combustion Engineering has been carrying out development for several years. I cannot do that, however, without producing a discussion which sounds like an advertisement for the Combustion Engineering advanced control system, and I believe that to be inappropriate in a document which may appear in the public record of your committee's deliberations. I will therefore answer briefly, and attach, for your further information, a document describing the Combustion Engineering development, which was prepared by Mr. John E. Myers, Director of Systems Engineering, Nuclear Power Systems.

The operators' performance can be improved by two design techniques:

- Human engineering of the operator's interface with the power plant to optimize his comprehension of the status of the plant processes.

Answers to Questions - J. R. Dietrich

- Optimization of some of the routine tasks to give the operator more time for concentration on the more important aspects of his job.

Human engineering encompasses the reduction in complexity of the information presented to the operator and optimization of the method of data presentation. Complexity can be reduced by combining several instrument outputs to yield the information which is of direct concern to the operator. For example, reactor power level and power distribution measurements can be combined to present to the operator the maximum linear power density in the reactor fuel, one of the quantities upon which operating limits are imposed. Or reactor power, power distribution, coolant flow, coolant temperature, and reactor pressure data can be combined to determine the margin available to the limit on departure from nucleate boiling. A major step toward optimization of data presentation can be made by the effective use of cathode ray tubes. These displays can take the form of printed statements, numerical data, graphs, or simplified system diagrams. In arriving at the optimum display one must take into account such things as the use of colors, the symbolic format, the physical orientation of the display, the information density, and the techniques for updating the information and displaying trends.

A number of routine tasks of the operator can be automated, but perhaps the most important area of automation is in the surveillance of the operability of the plant safety systems. A system can be designed, for example, to monitor the alignment of pumps and valves to assure that a given safety system is always ready to perform its function if needed. Misalignment can be enunciated for the operator and the misaligned components identified. Computer based systems can also be designed to assist the operator in the alignment of pumps and valves for periodic actuation testing, and to assist in the realignment into the "ready" condition after the test has been completed.

Question 6

Discuss the need for a "Swat Team" composed of people from industry, the utilities, NRC, etc.

Answer

I believe that a team of general nuclear experts, available to respond quickly in an emergency, would be very helpful. It should be composed of people chosen for the depth and breadth of their knowledge in the pertinent areas of nuclear plant design and operation, and should serve in an advisory capacity. I do not think it is advisable to have an outside team, whatever its composition, "take over" the operation of a plant that is in trouble.

The formation of teams, however, is only part of the necessary preparation for emergencies. Attention must be given to defining the roles of the teams, and to providing those things necessary for the team to do its job: working space; effective means of communication, both with the plant that is in trouble and with the home offices of the members of the team; adequate drawings and other design

Answers to Questions - J. R. Dietrich

data on the plant in question; reference books, related library facilities; etc. These and other aspects of emergency response are receiving concentrated attention from the Emergency Response Subcommittee of the Atomic Industrial Forum Policy Committee on Follow-Up to Three Mile Island.

Question 7

What are the advantages and disadvantages of standardizing the design of nuclear power plants? What would be the attitude of equipment manufacturers and plant constructors to standardization?

Answer

I believe there are great advantages, with respect to safety, reliability and economy, to standardizing the design of a nuclear system produced by a given manufacturer or constructor. Complete standardization of this kind proves difficult in practice, however, because of changing licensing requirements and because of the problem of interfacing the NSSS design with the balance of plant design, which varies from one constructor to another. Nevertheless, I believe the degree of standardization that has been achieved has proved its value.

Standardization in the sense of a common design for all manufacturers and constructors is quite a different matter. With regard to acceptance of the idea by system suppliers and constructors, I can only guess. If the concept had been proposed in the very early stages of nuclear power development it might very well have been accepted, but I can see great complications in implementing it today. Each NSSS vendor has spent many millions of dollars developing his designs, and each, no doubt, considers his the best. I believe there would be great reluctance to eliminate competition from the design process. Moreover, in a standard design, some design features would no doubt be selected from one supplier and some from another. How would one ever settle the question of who pays royalties to whom, and how much?

My own opinion is that a standard design of this kind would not be a good idea, for the following reasons.

- Presumably decisions as to the standard design characteristics would be made by some government agency. The government would, in effect, be designing the plant. I do not believe this is the way to arrive at either an economic plant or the safest plant.
- The addition of and improvements within safety systems has been and will continue to be an evolutionary process as designs change and knowledge grows. I am afraid this process would stagnate under the standard design concept.
- If all suppliers and constructors worked to a common standard design there would be no incentive to maintain the large, highly skilled design teams that exist today. We would lose our most valuable resource for safe design and for recovery from accident conditions.

Answers to Questions - J. R. Dietrich

- The design depends not only on how the components are put together, but on the components themselves: we would have to have standardized component designs as well as standardized system designs. I would expect that the number of sub-suppliers of items like pumps, valves, and motors would decrease if all had to manufacture to a common design. The nuclear business is not large enough for such sub-suppliers to justify re-tooling to a new design. Thus competition would decrease and along with it the pressure to supply reliable equipment.

Question 8

Should there be a standard design for control rooms and for the layout of control panels?

Answer

As is often the case, standardization of control room design and layout would likely be a mixed blessing. However, a certain level of standardization could probably be adopted which would yield most of the desirable effects, while minimizing the undesirable ones.

It seems reasonable that if the monitoring, control, and protective needs of power plants are similar, then the general layout of instrumentation and controls within the control room should also be similar. The arguments for this conclusion include:

- If there is a truly optimum design approach it should be used generally.
- Given standardization of general control room layout, more of the various design efforts being pursued would couple synergistically rather than being incompatible.
- Operations and other essential workers could more quickly perceive the nature of operations within a control room with which they were unfamiliar.
- Operator training would be simplified.

However, the case for standardization deteriorates quickly when specific design features of the panels and consoles are considered. We are faced simultaneously with rapid development of electronics-oriented technology, and an information processing task within the power plant which makes use of this technology seem virtually mandatory. One of the clearest lessons from TMI, the need to inform the operator better, is best pursued by the use of advanced electronics technology. Standardization of detailed design features would be extremely difficult to achieve at any point in time, and even if achieved, could be expected to inhibit design improvements.

Answers to Questions - J. R. Dietrich

In summary some level of standardization of control rooms for similar power plants appears to be a desirable objective. The first step, however, should concern itself with the issue of drawing the line between general layout issues (where gains can be achieved), and specific design issues (where standardization could prevent or delay needed improvements).

Question 9

How should the design of the control room be improved?

Answer

Given the development of generalized control room layout standards as discussed above, the potential for remaining improvement lies principally in two areas:

- Presentation of measured data to the operator, and
- Correlation and analysis of measured data for the operator.

A common objective underlies both areas; i. e., facilitation of an accurate perception of plant status by the operator.

Considerable effort over a number of years has been directed toward improvement in these areas. The promising approaches are those cited in the answers to questions 3, 4, and 5.

Question 10

Do you believe that additional water in the steam loop of a PWR would enhance reactor safety, and if so, how much additional volume?

Answer

Additional water inventory in the secondary loop of the steam generator increases the time available to restore feedwater flow once it has been lost. Clearly one will reach a point of diminishing return with respect to safety once the water inventory has been made large enough to forestall the need to restore feedwater flow for several minutes. I believe many of the plants now operating with recirculating steam generators have water inventories large enough that further increases would not provide a worthwhile increase in safety. However, I have not yet seen a formal analysis of this question. Once such an analysis is made judgements can be made with respect to individual plant designs.

Question 11

Do you believe two steam generators are adequate for a 1000 MWe plant? If not, how many generators would be appropriate to enhance safety?

Answer

I believe that two steam generators, if properly designed and constructed, are adequate for plants of capacity up to the maximum licensable under current

Answers to Questions - J. R. Dietrich

NRC rules (3800 MWt, corresponding to about 1300 MWe). From the point of view of redundancy of shutdown heat removal capability two steam generators are as acceptable on a 1300 MWe plant as on a 600 MWe plant. In absolute terms I believe that this redundancy is adequate, since operation is not permitted if there is substantial degradation of steam generator integrity. The only postulated transient I know of whose amplitude is larger in the case of two steam generators than in the case of a greater number is the steam line break accident. The effect to be countered is an increase in reactivity due to the cooling of the primary system water: this is accomplished by dropping the control rods. The somewhat greater reactivity swing which characterizes the two-steam-generator case is not important if adequate control-rod reactivity worth is provided, as it is. Again, the power capacity of the plant is not an important factor—a large plant with two steam generators behaves much the same as a small one under steam-line break conditions.

Question 12

Although it has nothing to do with TMI, what is your professional opinion regarding the potential for a reactor to run "out of control" if the fluctuation in nuclear fission activity should begin to oscillate in sympathy with mechanical vibrations or temperature deformations in reactor components?

Answer

I believe there is essentially no potential for a reactor to run "out of control" through sympathetic oscillation. The only coupling between reactivity and mechanical vibrations or deformations of components outside the core would be by way of the moderator temperature coefficient of reactivity. That coefficient is not large enough to produce large reactivity swings under any circumstances of mechanical vibration or deformation that I can imagine. Moreover, the negative Doppler coefficient of reactivity provides a very strong damping factor against reactivity oscillations. Finally, the period of any sympathetic reactivity oscillation would be several seconds long because of the thermal time constant of the reactor fuel and because of the transit time of water around the primary circuit. Consequently the control rods would have ample time to shut the reactor down following a reactor trip on high power level, even if a large amplitude oscillation could occur, and I believe a large amplitude oscillation is impossible except as a result of xenon fluctuations which are extremely slow, with periods of several hours.

Question 13

What is your opinion of a reactor control system that could be interrupted with a simulated accident problem without the operators knowledge? (During this period, the reactor would be operated by a computer and if during that time a real problem arose, the simulated problem would be automatically dismissed.)

Answer

The use of such a reactor control system would lead to undesirable consequences. The only benefit would seem to be that new data would be collected on the performance of individual operators under stressful conditions. There are two strongly negative factors: first, operator response to an actual accident might

Answers to Questions - J. R. Dietrich

be degraded; and second, some degradation in reactor control system reliability would be expected due to the substantial increase in system complexity and equipment sophistication.

Moreover, operational experience during transient conditions has shown operators to be relatively calm under stress. Errors seem to most often result from either the inability to properly interpret the data presented, or from an imperfect understanding of the consequences of specific actions. We would expect the error probability to be particularly high during the course of a "real accident," if it were to interrupt a "simulated accident" of a different nature—the sequence of simulated and real behavior would be highly confusing to the operator.

Question 14

Regarding the man/machine relationship, what are the pros and cons in operating a reactor from a small control console where status and trend data can be read on a terminal on command.

Answer

Operation of the reactor from a relatively small console is both achievable and desirable. Console size would necessarily be larger than a single terminal to avoid completely unacceptable information density. For example, the master control consoles in some recent C-E plants are U-shaped and sized to mount ten cathode ray tubes. This results in approximately a 14-foot span between wings. Controls for plant operation from hot standby to full power operation are located on this console. During accident situations, total plant status information is available from the console, but auxiliary panels within the control room may house the necessary controls for actuation of appropriate plant equipment.

J. E. Myers
SYS-A-013
June 19, 1979

Page 1 of 4

INFORMATION PERTINENT TO QUESTIONS 3, 4, AND 5

Operation of a commercial nuclear power generating station requires the surveillance of several thousand pieces of instrumented data. The station operators are responsible for providing this surveillance and for making control decisions based upon this data in a safe, economic manner.

Technological tools are available within the "state of the art" to reduce the complexity of the operators surveillance tasks and to enhance the operator's comprehension of the data. Technology is not available to replace the operator in the overall plant control/decision making role. The human brain, with its unique abilities to learn and to extrapolate, is required to effectively monitor and control the complex, interrelated processes of a nuclear power plant.

There are two key areas where current technology can improve the operators performance:

Human engineering of the operator's interface to the power plant to optimize the operator's comprehension of the status of the plant processes.

Automation of certain elements of the routine daily tasks to free up the operators time to concentrate on the more important aspects of his job.

HUMAN ENGINEERING

C-E has performed research on the human-engineering aspects of the operator-process interface. In its studies C-E concentrated on two basic areas: the reduction in the complexity of the information presented to the operator, and in optimization of the method of data presentation to the operator.

Reduction in Information Complexity

The goal of reducing information complexity is one of reliably "condensing" several instrumented data points into a single index that provides all of the pertinent information on the actual plant parameter of interest. This goal is achieved in a two-step process. The first step is to systematically analyze the various processes of the plant to determine candidates for condensation. The second step is to implement a scheme to reliably automate the "condensation" process.

J. E. Myers
SYS-A-013
June 19, 1979

Page 2 of 4

An example of this condensation process is the Core Operating Limit Supervisory System (COLSS) that is implemented on recent C-E plants. COLSS is an integrated reactor core supervision system that is implemented in a digital computer. COLSS monitors several hundred measured process parameters and condenses these measurements into three easily understood performance indices that are displayed and alarmed to the operator on-line, in real time.

Another example is the hierarchical display and alarm system that is the major operator interface in C-E's most recent control room designs. In this hierarchical arrangement, all plant systems are categorized in a hierarchy that parallels the operators's hierarchy of tasks. This system is implemented with multi-color cathode ray tubes (CRTs) and digital computers.

The three tier hierarchy has at its top level a monitor display. This monitor display provides a condensation of the status of all subsystems and components in a major plant process. Alarms and anomalies on a lower tier trigger alarm behavior on the monitor level that highlights the affected system, and cues the operator automatically to the next lower tier display that provides greater detail on the alarm situation.

On the next tier below the monitor display are the control displays. Each of these displays contain the information required to effect control of a major plant process or component. Data related to the control evolution are also displayed for operator convenience. The control displays also provide a level of information condensation. Component symbols provide alarm behavior based upon the status of a number of measured data points represented at the lowest level of the hierarchy. The operator will receive an automatic alarm cue to the next lowest level if pertinent alarm information is contained there.

The diagnostic displays reside at the lowest level of the hierarchy. These displays contain all the information that is monitored on any particular component or subsystem.

The operator can maneuver "vertically" through the display hierarchy, "zooming" in on a problem; or "laterally" through the hierarchy, scanning related systems and processes. The operator can also jump directly to any display in the hierarchy without traversing the intermediate displays. The operator interface device for display selection is a simple keypad, similar to a pushbutton telephone from

J. E. Myers
SYS-A-013
June 19, 1979

Page 3 of 4

which he can easily traverse the hierarchy, assisted by the automatic computer cueing.

Optimization of Data Presentation

C-E's research has indicated that a critical element in improving operator performance is in tailoring the presentation of displayed data to human characteristics. Computer technology has provided flexibility in information encoding techniques that allow the presentation of data to be optimized to both the operator and the specific task he is expected to perform.

In C-E's studies, color, blink, symbolic format, physical orientation on the display, and information density and update technique are all used to encode display information to increase the operator's comprehension and performance. The system is designed to highlight color abnormalities and anomalous readings by changing the shape and format of the data when the reading reaches a preset limit. C-E studies have shown that a great amount of information can be condensed into a single display. However, these studies indicate that reduction of all necessary information into one display is not practical with current methodology or technology. A great reduction of necessary display area is possible, and is the cornerstone of our most recent control room arrangements.

These state-of-the-art control room arrangements address many human engineering factors in addition to those related to CRT displays. The design methodology includes consideration of criteria on such variables as maximum distance between any two control functions, minimum distance between separate control devices, viewing angles, number of operators required (normal operation, startup, shutdown, and accident conditions), and access by non-operator personnel.

Panel layout concerns such as functional groupings, symbols, left to right organization (heat source to heat sink in current designs), and color representation have been addressed and standardized where practical. In most of these areas, human engineering factors are adequately defined and may be implemented in a straight-forward fashion. Another area that has received additional attention is that of "seldom used controls". These are the controls the operator might be required to use in an accident or other abnormal operating condition. Methods to better guide the operator in these situations are incorporated in the design of the panel layouts and the related data presentation.

J. E. Myers
SYS-A-013
June 19, 1979

Page 4 of 4

All of these factors must be integrated into the control room design process in order to obtain the maximum advantage from computerized information processing and display systems.

AUTOMATION

The second key area of potential improvement in operator performance is the automation of selected tasks to remove some of the surveillance burden that the operator is required to perform.

The most pertinent area of automation is that required for surveillance of the operability of the plant safety systems.

C-E is implementing a system to monitor the alignment of pumps and valves in response to NRC Regulatory Guide #1.147. This system will provide annunciation to the operator if misalignment of an instrumented pump or valve occurs. We are also developing a computer based system to assist the operator in alignment of pumps and valves for periodic actuation testing. This system provides positive indication of correct system alignment for test and positive indication when post test realignment is achieved. Hard copy test documentation is then produced of test results and correct system alignment.

C-E has implemented systems that automatically monitor the status and operability of the Reactor Protection System. When problems are detected, annunciation is provided to alert the plant operations staff. However, restrictions placed on the implementation of these systems by interpretations of existing regulations has had the effect of stifling industry impetus to develop these automated monitoring systems. A more realistic approach in the NRC evaluation of the safety significance of these systems is required.

CRT Displays for Power Plants

M. M. DANCHAK
 Combustion Engineering, Inc.

Color CRTs with graphic capabilities certainly have complicated the task of display design. Designers now have to worry about color assignments, contrasting, symbols, blinking and a host of other variables. The author offers guidelines for effective color CRT display design, concentrating on the human factors aspects of various techniques.

DISPLAYING POWER PLANT data on multi-colored, computer driven CRTs provides the potential for raising operator-machine interfaces in these plants to new heights. The amount of detail and flexibility inherent in color CRT displays promises better and more timely information. However, the mere existence of such promises adds little to a power plant control room. The critical task is the exploitation of this potential in an intelligent manner. Technology has removed many constraints from the machine portion of the interface. Equal effort must now be placed on the human aspects.

Although the eye can sense all the information on a CRT face, the brain cannot begin to act on that amount of detail. Some mental processing must take place before any information can be entered into human memory. This usually involves some form of feature extraction and/or pattern recognition on the operator's part to encode correctly the information for internal storage in short-term memory. Such storage is the initial step in display comprehension.

To aid this mental process, a determined effort must be made to keep each display as clean and unobtrusive as possible. This effectively reduces

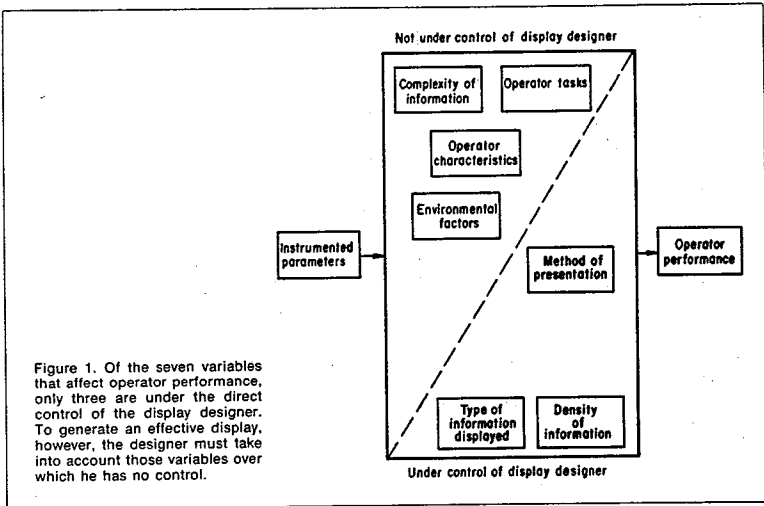
the noise level of the display and consequently decreases the human search and processing time required for information detection and comprehension. An effective display should not require any conscious effort for analysis on the part of the operator. He must be able to immediately grasp the situation and take appropriate action.

A designer of CRT displays that satisfy these criteria must have a thorough understanding of the power production process, display techniques and, most importantly, the operator. Such total understanding is seldom found in a single individual. This article offers guidelines that permit users, who are familiar with power plant operation but not specifically knowledgeable in display techniques, to create effective CRT displays.

Performance parameters

Optimization of operator performance entails an appreciation of the variables that influence an operator and variables that can be influenced by a display designer. Operator performance has been defined (Ref. 1) as a function of several variables:

- complexity of information
- operator tasks
- operator characteristics
- environmental factors



- type of information displayed
- density of information
- method of presentation.

Although all of these may impact operator performance equally, the degree of influence a display designer has on each variable is very subjective. Figure 1 illustrates the grouping of these variables in power plant applications. Typically, the operator is required to monitor large numbers of discrete parameters. The complexity of information and operator tasks are predetermined and therefore not under the control of the display designer. Likewise, he has little or no input in determining operator characteristics or environmental factors. The designer does, however, have a large and often sole impact on the remainder. He must decide what to display, how much of it to display, and the most effective format in which to present it so as to maximize operator performance.

Operator tasks

Analysis has shown that the operator is involved in three major tasks: monitoring, control and diagnostic. Unfortunately, these areas are too broad to base guidelines upon, since each entails many sub-

tasks. Five tasks, however, have been identified (Ref. 2) that appear basic to CRT display reading and may be appropriated to serve as generic sub-functions. These five tasks are: identify, search, count, compare and verify. Table I illustrates their meaning in the context of the power production process and lists them in descending order of frequency.

The search task is performed at all times, since an operator is never concentrating solely on the CRT. He must find the target before processing the information according to one or more of the other tasks. Identify, the simple act of recognizing the target, also is required in all instances. It is often difficult to separate search and recognition tasks, since both are involved in bringing the operator's attention to the correct target. Only after successfully completing these functions can he begin to process the information. Processing then involves the tasks of comparison, verification and counting.

This implies that a designer should optimize the display for search and recognition and then satisfy criteria for the remaining tasks. This is a restatement of requirements for a "clean" display men-

tioned previously. Regardless of how important a parameter is, it becomes noise when the operator is looking for something else. Anticipating operator needs is an extremely difficult assignment. One is more inclined to use the saturation approach—display everything. But this is self-defeating in the long run. The primary maxim of effective display design is to give the operator what he needs, only when he needs it.

Informative coding

Information displayed on a CRT is often coded according to various schemes. The English alphabet represents a coding scheme in that an entire concept may be represented by one or more letters. Numerics is another example of coding in which quantities are depicted by a string of digits. Symbolology is a third example, where unique arrangements of lines and curves depict pumps, valves, transistors and other components. The question here is how to best code information to accomplish a given task. Since the definition of information is "knowledge that was not previously known," many items such as labels do not necessarily qualify at all times.

Human factors literature abounds with treatises on abstract coding methods (Ref. 3) that use single letters, digits, shapes or colors to depict complex ideas. While much of this data is directly applicable, a large majority must be treated cautiously. A random string of alphabetic characters such as "uppm" may be used abstractly to represent the concept of a device that transfers fluids by suction or pressure. One may use this coding scheme to obtain search and identify task response times. A rearrangement of these letters to form the string "pump" would result in quite different times due to operator familiarity. The point is that each area

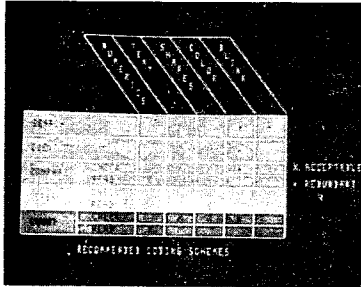


Figure 2. A variety of coding methods are available, but some methods are more suitable for certain operator tasks than others. Recommended coding methods are indicated by an "x", while the asterisk indicates redundancy.

of application has its own convention and coding biases that are not abstract. Human factors research provides excellent data that must be judiciously extrapolated to individual areas of concern.

Such an extrapolation yielded five applicable coding methods: numeric, textual, shape, color and blink. Although these agree in philosophy with basic human factors definitions, some modifications were made. Numerics refers to digital strings representing some measurable value of a parameter such as temperature or pressure. Textual coding connotes alphanumeric strings arranged to form a meaningful word or words common to the power production process. Logical abbreviations of words also qualify under this scheme. Shape encompasses standard power process symbols (pumps, valves) as well as geometric objects (bars, columns). Color and blink have been shown to be most effective when used as redundant codes (Ref. 4-6). This means that color and blink should be used to reinforce information coded by other means, such as blinking a pump symbol in an alarm color.

Figure 2 is a summary of recommended coding schemes for power production CRT displays. Each task has associated recommended coding methods indicated by a checkmark. Compare, verify and count tasks are further subdivided into "check" and "read." A check subtask is one that has a discrete number of status states (on/off, open/closed), whereas the read subtask has variable states, such as the value of a fluid temperature. Reading involves more mental processing since

Table 1: Operator Generic Subtasks

Subtask	Question type	Example
Search	Where is?	Where is the flashing symbol?
Identify	What is?	What does the flashing symbol represent?
Compare	Yes/No	Is the flow equal in both coolant loops?
Verify	True/False	The oil lift pump has been actuated
Count	How many?	How many valves are open in the letdown line?

people have a tendency to "vocalize" what they read. Perceiving a status does not require this translation.

Test and shape coding should be used for the search and identify tasks. Successful completion of these tasks results in focusing the operator's attention on a specific portion of the CRT—they do not involve processing the information located there. A pump symbol, perhaps with amplifying text, easily allows the operator to find the correct pump on the display. Likewise, the name of a parameter will accomplish these tasks provided the operator knows what he is looking for, as in an operator initiated search. Computer initiated searches occur under alarm conditions, when a parameter has exceeded its accepted value and the operator must be informed. In situations such as this, color and blink are at their best since attention-getting is required.

The status checking subtask is similar in comparing, verifying or counting tasks. Since only a small number of possible states exist, status checking is quick and requires simple coding methods. A symbol that has few possible configurations is ideal in this case, particularly when color is used to reinforce the status message. For example, a circle with the circumference colored may be used to indicate one state while the same circle with both the circumference and interior colored indicates another. A unique color for each state further enhances the concept.

Reading subtasks require the acquisition of very specific information from a large number of possibilities, such as one temperature out of a possible range of hundreds. Within the context of information theory, this represents more information than a status check. Hence, one must pay the price of

more lengthy processing. The only feasible means of coding this information is numerics. Once the information is assimilated, the operator performs his comparison, verification or counting. It should be emphasized that color is not used as a code in relation to these tasks. The color of the numerics may change to indicate an alarm, but this is done to aid the search task. Legibility and contrast are the only color considerations and do not constitute coding in the real sense.

Colorful conventions

As mentioned earlier, the display designer must conform to conventions in the application area to make coding easier. Numerics, text and shapes should be familiar to the operator. What may seem unnatural in one application may be perfectly logical in another. This is particularly true for color coding.

Red and green are often used in the power industry to indicate on and off respectively. This poses a problem for the display designer because he may think of red as a danger color. Does he use red to indicate both conditions, does he select a different color for danger, or does he try to change the convention? How does he reconcile this in light of proven human factors data? This problem may be alleviated if he remembers that he too has been biased. Everyday life has programmed him to respond to red as danger just as the operator's job has trained him to respond to this color as "on." The operator may function under a double standard, red meaning "on" while operating the plant and meaning danger while driving his car. Changing the convention or using the same color for both conditions will surely introduce confusion. The criteria for alarm colors is that they be unique, logical and fit within existing standards.

Color CRTs further compound the problem in that any item drawn on the screen must be in some color to be perceived. Table II represents one solution for a color CRT that accounts for prior conventions, search criteria and legibility requirements. Black is the unactivated screen color and serves as a logical background. Dark blue lies far below the eye's spectral sensitivity peak and may be difficult to perceive when the eye is stimulated by other colors on the CRT. This is used to advantage for labels and other purely advisory status items. If the operator wishes to read the label associated with a variable, it becomes information. Otherwise it is noise. The poor contrast of blue on black reduces the noise impact but still allows the label to serve as information when the operator focuses on it. Cyan (light blue) has a contrast ratio close to white but avoids the greater stimulus from the longer wavelength components of white. The

Table II: Recommended color codes

COLOR	USE
RED	ON-ENERGIZED
GREEN	OFF-UN-ENERGIZED OR DEENERGIZED
CYAN	INFORMATION BEARING NUMERIC DATA OR TEXT
BLACK	OFF-DE-ENERGIZED, CLOSED, NORMAL
WHITE	INTERMEDIATE BETWEEN GREEN AND RED
YELLOW	CAUTIONARY-ATTENTION REQUIRED
BLUE	CAUTION-TO BE USED SPARINGLY

corresponding legibility of cyan makes it applicable for numerics and alphanumeric text that always contain information.

Red and green retain their conventional on/off definitions while white is used as an intermediary between the two. Thus a variable speed pump symbol would be colored green when off, red when fully on, and white when partially on. Yellow and magenta provide logical alarm colors as well as excellent contrast with black for portrayal of necessary alarm information. Also, their uniqueness aids the search task.

Blinking should be used only for attention-getting in the search task. A single blink rate between 2 and 5 Hz should be used in all instances and the number of items blinked at a given time must be held to a minimum. The attention-getting value is greatly diminished when more than one display area is blinking. Also, blinking degrades legibility, making value reading difficult (Ref. 7). If the parameter value is blinked for attention-getting, some means must exist to stop the blink prior to processing that value. An acknowledge function satisfies this criterion nicely by allowing the operator to respond prior to evaluating the information. Otherwise, blink the area near the parameter, but not the value itself.

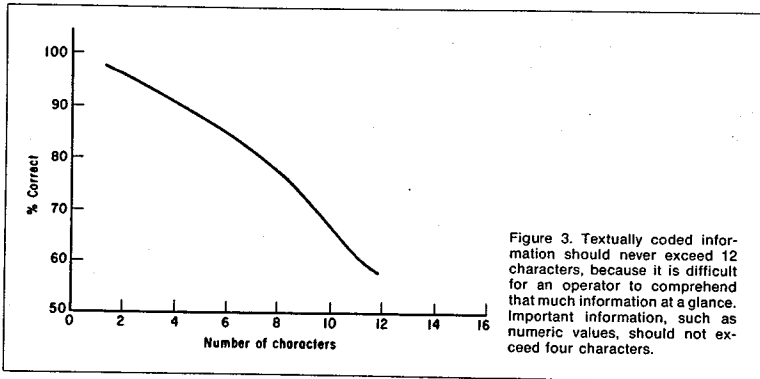
Overloading the screen

Information density involves determining how much data can be placed on the screen before the amount begins to adversely affect the operator's

ability to perform his basic tasks. Ideally, one expects a single information/unit area figure based on a detailed information theory analysis. In the practical world, there are too many variables to make such a figure useful and one must settle for intuitive results tempered by psychophysical data. Advice given in this section assumes a 19-in. (48.26 cm) diagonal CRT located 28 in. (71.12 cm) from the operator. The span between the operator and the CRT is the optimum viewing distance for a CRT of this size (Ref. 8) and within the operator's reach (Ref. 9).

The cleanliness of a display determines the operator's ability to successfully perform his search and identify tasks. When he scans the display for a specific parameter or target, all other information on the screen is noise. It is intuitively obvious that an upper limit exists on the amount of active screen area. Quantifying this is another matter. Experience shows that display loading (the percentage of active screen area) should not exceed 25 percent. This may seem extremely low until one considers that a well-designed page of printed material has a loading of only 40 percent (based on the author's analysis of the journal cited in Ref. 1).

An analysis of existing CRT displays that were qualitatively judged "good" revealed a loading on the order of 15 percent. The remaining area constitutes "white space" that is essential for clarity in any display. Furthermore, the amount of variable data on these displays never exceeded 75 percent of the total active area. The product of these limits dictates that no more than 18.75 percent of the



screen should contain information of continued interest to the operator.

Density within the display is also an important consideration. One would like to know the maximum number of characters, the appropriate symbol size, and proximity to other information areas. The average visual angle for central foveal vision is quoted at 5 deg (Ref. 10). Stated more clearly, when one fixates on a point, one sees information within a 5-deg solid cone to 50 percent accuracy. This 5-deg angle is also called the "span of attention" and is an important parameter that has great impact on display design.

Figure 3 illustrates the practical application of this psychophysical fact. The operator's attention span translates to 2.44 in. (6.21 cm) measured on the screen face. A survey of various display vendor data indicates that the average character width, including allowance for character spacing, is approximately 0.2 in. (0.5 cm). When arranged horizontally, 12 characters can fit within the 5-deg cone. Hence an operator can see a maximum of 12 characters at a glance. To improve accuracy, textually coded information should not exceed 6 characters, although labels can be up to 12.

Numerics usually require more accuracy since they are heavily laden with information. Therefore, numerically coded information should never exceed 4 digits without good cause. This produces an average reading accuracy of 90 percent without being overly restrictive. In all cases, the horizontal arrangement of characters is preferred to the vertical (Ref. 11).

Since the span of attention defines discrete areas of the CRT, it is advisable to have each area contain only one piece of information. One would want to separate fixation points of different parameter values (i.e., pressure and temperature) by 2.44 in. (6.21 cm) so the operator sees one idea with each glance. Likewise, two parameters that are consistently compared should both fall within the same span. This explains why the best arrangement for comparison is the columnar form.

To minimize the number of characters in a word, abbreviations can be used when necessary. If an accepted abbreviation does not exist, one can be fabricated using the concept of masking and/or vowel deletion. The first and last few letters of a familiar word are seen more clearly than interior characters. This is predominantly due to the proximity of white space on either side of these letters while the interior is effectively masked by other letters. Within the context of the power production process, TEMP is an accepted abbreviation of "temperature" while masking can be

applied to "boiler" to yield BOLR and still retain the meaning. Another technique of abbreviation is to delete vowels, as in "condenser" and CNDNSR. (Caution: Such abbreviations should be tested prior to their use.)

A final point deals with the placement of information on the screen. When the operator turns his attention to a specific CRT, his initial fixation point naturally falls at the center. Does he search the screen from this point in any predetermined manner? It has been shown that search times are significantly faster than the average for targets in the upper right quadrant and slower for those in the lower right (Ref. 12). No difference exists for the left two quadrants. These findings can be used to advantage by placing the most important information in the upper right quadrant and the least important in the lower right.

Recommendations for information density are summarized in Table III. Obviously, these are general in nature and should not be used blindly. The display designer must balance them against his experience for each and every display.

Selecting a method

Method presentation, which deals with organization of the overall display, is the final variable

Table III: Recommended Density Values

Total display loading	
Maximum:	25%
Dynamic display loading	
Maximum:	18.75%
Text word size	
Maximum:	12 characters
Recommended:	6 characters or less
Numeric word size	
Maximum:	12 characters
Recommended:	4 characters or less
Symbol size	
Maximum:	2 in. (5.08 cm)
Recommended:	1 in. (2.54 cm)
Word Orientation	Horizontal
Word spacing	2 in. (5.08 cm)
Preferred quadrant (in order of preference)	Upper right Upper left, lower left Lower right

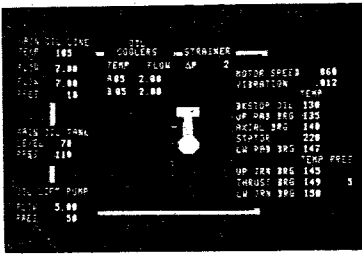


Figure 7. If the motor section of pump 2A has a problem, the operator can request a diagnostic display which provides all pertinent information in alphanumeric form. Information on this display is grouped functionally and interrelationships are shown with connecting lines.

tions in Table III. Since CRT displays are used to indicate plant operation, dynamic data are of utmost importance. The designer must now evaluate his display in terms of rates of change and how well these changes can be detected. This procedure is part of a design methodology.

Designing displays

Determining the purpose of a particular display is the first step in display design. Each variable that will appear on the display should be justified, in writing, on a display form. Display design forms should ask both philosophical questions of the designer (purpose, special considerations) and specific questions regarding particular parameters that need to be displayed.

Since the determination of specific display parameters is the end result, it should be specified first. Then, and only then, should the proposed display be analyzed to determine if sufficient data exist to yield the desired result. The input must never define the output. This ensures a fresh look at the system by the user with current technology in mind. Historical reasoning (we always did it that way), while valuable for confirmation, is a poor base on which to build a new design.

Filling out design forms defines what is to be done, not how. Details on how the output accomplishes its objective is determined next. Given a defined output, the designer then decides which display category is most applicable. Here the guidelines come into play, as shown by the recommendations of Figure 4. After deciding on a display method,

the designer has a number of detailed items to consider: arrangement, size of active display area, color assignments, abbreviations, character size and spacing, level of detail, type of coding, parameter placement and rates of change, to name a few.

Designing effective CRT displays is both a formidable and confusing task, requiring the designer to gain expertise in unrelated areas of technology. Guidelines are of little use, however, unless the person applying them is intimately familiar with his particular application process. Guidelines presented in this article are intended to provide an experienced user with advice in areas that are outside his specialty.

The level of sophistication of both instrumentation and display techniques has risen rapidly in the recent past and will continue to do so. Man, however, has changed little and is not likely to do so. Therefore, electronic display devices must be tailored to man rather than have him tolerate fancy but ineffectual equipment.

References

- Hitt, W. D., et al, "Development of Design Criteria for Intelligence Display Formats," *Human Factors*, Vol. 3, 1961, p. 86.
- Hitt, W. D., "An Evaluation of Five Different Abstract Coding Methods—Experiment IV," *Human Factors*, Vol. 3, 1961, p. 120.
- McCormick, E. J., *Human Factors Engineering*, McGraw-Hill, New York, 1970.
- Anderson, N. S. and Fitts, P. M., "Amount of Information Gained During Brief Exposures of Numerals and Colors," *Journal of Experimental Psychology*, Vol. 56, 1952, p. 362.
- Jones, M. R., "Color Coding," *Human Factors*, Vol. 4, 1962, p. 355.
- Smith, S. L. and Goodwin, N. C., "Blink Coding for Information Display," *Human Factors*, Vol. 13, 1971, p. 238.
- Smith, S. L. and Goodwin, N. C., "Another Look at Blinking Displays," *Human Factors*, Vol. 14, 1972, p. 345.
- Dreyfuss, H., *The Measure of Man: Human Factors in Design*, Watson-Guipill Publishers, New York, 1967.
- Morgan, C. T., et al, *Human Engineering Guide to Equipment Design*, McGraw-Hill, New York, 1963.
- Woodworth, R. S. and Schlosberg, H., *Experimental Psychology*, Holt, Rinehart & Winston, New York, 1954.
- Woodward, R. M., "Proximity and Direction of Arrangement in Numeric Display," *Human Factors*, Vol. 14, 1972, p. 337.
- Baker, C. A., et al, "Target Recognition on Complex Displays," *Human Factors*, Vol. 2, 1960, p. 51.

MICHAEL M. DANCHAK is a Principal Engineer for the Instrumentation & Controls Engineering Div. of Combustion Engineering, Inc., Windsor, CT. Article is based on a paper presented at the ISA Power Industry Division Symposium, San Francisco, 1976.

THE MAN-PROCESS INTERFACE USING
COMPUTER GENERATED CRT DISPLAYS

Michael M. Danchak,
Supervisor, Display Systems
Instrumentation and Controls Engineering
Nuclear Power Systems
C-E Power Systems
Combustion Engineering, Inc.
Windsor, Connecticut

INTRODUCTION

The past few years have seen exponentially increasing interest in the area of human factors by the process control field in general, and the power generation industry in particular. The seventh decade of the 20th century started with a smattering of papers on the subject, as related to control rooms, and expanded to a formal review by the Electric Power Research Institute⁽¹⁾ completed last year. All the literature criticizes the fact that existing power plant control rooms were designed based on the "leftover" policy. This attitude allocates functions to the operator only when it cannot be accomplished by hardware. Furthermore, these "leftover" functions received little or no attention by the designers, assuming the operator would soon learn to cope with the given system. Although this evaluation may be a bit unsympathetic towards the previous generations of control room designers, the fact remains that existing systems do not adequately account for the human in that system.

Fortunately, most of the publications do not dwell on the deficiencies of the past, but expound the virtues of the systems of the future -- the so-called "advanced control centers." These are radical departures from their predecessors, using recent technological advances to acquire and display information about the power generation process. Computers, multiplexing equipment and Cathode Ray Tube (CRT) displays are becoming the norm rather than the exception. Attendant with these hardware advances are concerns for the operator and his ability to function in this environment. More than words, however, must be expended to exploit the potential of this new technology. Control room designers are currently presented with a rare opportunity in which they may "atone for the sins of the past." This is possible by intelligently accounting for the attributes, both good and bad, of the human operator. Design of the control and display systems must be done with the operator primarily in mind.

While the new developments in technology are invaluable, one must proceed with caution. The application of interactive computer graphics to problem solving tasks has made great advances in areas such as computer aided design. One is immediately tempted to apply similar techniques to power plant control rooms. Systems have been devised that require all interactions between the process and the operator to occur through the CRT display itself⁽²⁾. Other systems are much more cautious and merely use the CRT to duplicate the functions of the many dials and meters previously used for information display.

Both extremes have shortcomings due to poor display design. Insufficient experience with display design and knowledge of the functioning of the human operator precludes direct interaction with the screen at this time. Duplication of previous display methods does little to aid the operator in digesting the voluminous data. This technique also maintains discreteness of parameters rather than integrating them into the overall process. Controls and displays should remain separated until effective CRT display systems have been developed and proven successful. The display system design is the quantum jump in the operator interface. Direct operator interaction may easily follow, if deemed desirable, once the display system has been made effective.

The major problem associated with displays is two-fold; the display set organization must take an integrated approach to the power generation process and each display page in the set must be based on sound human factors principles. The latter has been touched on⁽³⁾ and work is continuing on the details of effective display page design. This paper will concentrate on the problem of organization by analyzing the purpose of the CRT display system and posing a solution in the form of a display design methodology. The efficacy of this approach will then be demonstrated using a simple Nuclear Steam Supply System (NSSS) example.

MAN-PROCESS INTERFACE

The CRT display system is the operator's primary means of determining the status of the process he is trying to control. While the popular term "man-machine interface" may be applied to such interactions, the semantics are somewhat misleading. When one enters and receives information in an interactive graphics application, the interface is truly between man and machine (computer). However, in the process control field the operator is more interested in interacting with the process than with the computer. The intermediate machine aspects should be transparent to the operator to establish a man-process interface. One may consider this a trivial difference, but the designer and the user are certainly affected by that difference.

Displays must optimize the interface between the operator and the process, rather than the operator and the computer. The computer is merely an information pathway between the two. The display system is the operator's window to the process. As the analogy implies, information in this interface travels in one direction only. The operator views the process through the CRT screen and uses his separate controls to accomplish changes. In computer terms, the CRT is an output device, as opposed to providing both input and output. The man-process interface must be designed accordingly.

Establishing the terminology also established the purpose of the display system: to provide a decision making tool for the operator in relation to the process. The next question to be asked is, How is this done with the displayed information? How does the operator use the window for control? Models of human performance⁽⁴⁾ indicate that the operator maintains his own internal concept of the process and makes adjustments according to this replica. When the operator looks at the screen, he expects to find certain information that matches his model.

According to current theories of the human perceptual cycle,⁽⁵⁾ this model is called a schema. It determines the operator's predisposition to finding relevant data under various conditions. The anticipatory schema directs his exploration of the screen, from which he samples data and subsequently modifies his mental model. This cycle explains why we often overlook certain aspects -- they are totally unexpected. Another interesting point is that the data itself does not govern the subsequent behavior of the operator. It is the schema, or his hypothesis on the source or cause of this data, that determines what he does next.⁽⁶⁾ The exploration of information continues through repeated observations until the operator is convinced his hypo-

thesis is correct.

The task of the display designer is to aid the formulation and modification of this schema with relevant data. Displays must emphasize the unexpected and provide a means by which the operator can establish his hypothesis and either confirm or reject it based on related events. This model of the man-process interface verifies the problem areas stated previously. The individual display pages must be effectively designed to complement the operator's concept of the process and make the unexpected obvious. Furthermore, the interrelationships between the displays must be logically established to allow the operator to make the requisite observations quickly and intelligently. Display hierarchy is more than a convenient means of organization -- it is a vital tool in determining the operator's ability to react successfully.

DESCRIPTION OF THE METHODOLOGY

The emphasis of the proposed display design methodology is on integration of displays. When assigned to such a task, the designer typically asks the number of display pages to be created and proceeds from there on an individual basis. A better question is, How many displays does the operator need and how can they be logically related to satisfy these needs? Only then should the details of the individual pages be addressed. The methodology is devised to account for the model discussed in the previous section. The progression in detail also provides an inherent documentation package for each display page in the system.

Figure 1 illustrates the steps in the procedure. A display hierarchy is established by defining the purpose and function of the display set and each individual display. This should be done on a systems level that deals with major portions of the plant, such as the NSSS, main steam, feedwater, etc. The next step identifies the display parameters necessary to accomplish the purpose just specified. Note the heavy reliance on operating experience. This is done to ensure that the display system meets the operator's requirements. Once the output is determined, the displayed data is related to the input available to complete the input-output sequence. With this information in hand, the actual design of the individual display page is done according to human factors guidelines. The final step specifies the processing required to update the displayed data. Appropriate forms should be devised for each step on the procedure to formalize the process and ensure completeness and continuity. Each of these steps will be discussed in more detail in the following paragraphs.

Display Hierarchy

Coincident with specifying the purpose and function of each individual display page, one must establish a concept of how the pages are related according to the operator's schema of the process. A list of display page names must be drawn up and the interrelationships determined. This concept, or hierarchy, ensures an integrated approach and also determines the maneuverability between pages, as will be shown shortly. Such a unifying mechanism tests the effectiveness of the display strategy before time and effort is expended on detailed page design. Using the hierarchy, operations oriented personnel may postulate actions of the operator and determine where the required information can be found. Such a paper study improves the efficiency of the procedure without sacrificing flexibility or wasting engineering hours.

The relatively new field of hierarchical system theory⁽⁷⁾ offers a valuable guide in establishing the system structure. One must decompose the system into subsystems, and these subsystems into sub-subsystems, and so on, until a convenient amount of detail is reached. Decomposition may be done according to level, time, mode or other means applicable to the system of interest. The information structure is then defined by specifying the amount and type of information available to each component. Finally, the degree of coordination and data flow between the components must be determined. The basic techniques of hierarchical system theory will be used without resorting to mathematics or complex details.

A convenient and applicable level decomposition has been established during the analysis of operator tasks⁽³⁾. There is a direct correspondence between the monitoring, controlling and diagnostic tasks, the methods of presentation and the logical maneuvering between displays. Displays will henceforth be categorized as monitor, control or diagnostic. The hierarchy of this categorization is shown in Figure 2. The highest level display treats the monitoring task that provides an overall view of the system involved. Beneath this are multiple control displays that show major components of the monitor and provide information necessary to control that component. The diagnostic display contains all instrumented parameters related to that component, thereby allowing detailed diagnosis of any problem. The amount of detail inherently involved with the last level may require multiple pages of displays.

It should be emphasized that detection of anomalies is not restricted to diagnostic displays, only the level of detail is limited. Alarm indications are available

at all levels, as described later. Essentially the hierarchy defines levels of "zoom" for alarms where the operator moves to the level of detail necessary to determine the anomaly.

Given a set of displays, one needs a means of retrieving one particular page of the set for viewing. This establishes the maneuvering mentioned in previous paragraphs. An obvious method is to assign page numbers to designate each display and use the designator for retrieval. Assuming a non-trivial number, a directory is necessary to relate these number designators to the actual contents. The operator must scan the directory for the desired information, enter the assigned number and view the information on the CRT screen. Using this technique, an operator can randomly access any single page of the set rather easily, provided he knows the designator.

Another technique is to move sequentially through the set from some predetermined beginning. A wrap-around feature would display the first page after the last page in the sequence has been viewed. For added flexibility, movement through the set can be in either the forward or backward direction. Two simple function buttons are all that are required for retrieval. While this does not require a priori knowledge of page numbers, it requires retrieving an average of $N/2$ pages before finding the desired information, where N is the number of displays in the set.

A combination of the two methods is preferable. One can randomly access the desired page with the aid of a directory and then move sequentially through the set, as desired. This combined approach will be referred to as "paging." It retains flexibility, while decreasing retrieval times for displays in the vicinity of the page currently being viewed. This represents horizontal movement along the levels shown in Figure 2. Although one must put the pages in some sequence, the paging concept does not exploit the interrelationships of displays as defined by the hierarchical structure.

To take advantage of the inherent logical progression between levels, one should incorporate a second means of retrieval called "sectoring." This technique allows the operator to move vertically through the hierarchy with a minimum of effort. Simple operator actions allow him to move from the monitor level to a related display on the control level and still further to the diagnostic level, following one branch of the tree structure. Equally simple actions allow progression up the structure as well. While sectoring constrains the maneuverability to a limited number of displays, the allowable pages are logically related to the

current display. Furthermore, no directory or memorization is required by the operator if sector indicators are made an integral part of the display.

Maneuverability can be incorporated into the hierarchy by drawing boxes to represent each display page and assigning page numbers to each box, as shown in Figure 3. This number (204) would be listed in a directory with its associated name, and used to randomly access that display. Horizontal maneuverability is indicated by the "Page Back To" and "Page Forward To" entries, 203 and 201 respectively. These pages are on the same hierarchical level as the current page and are accessed using some forward/back selection mechanism. The sector numbers attached to the interconnecting lines represent the indicators that would appear on the display and that would be entered to move vertically in the hierarchy. Selection of Sector 1 or 2 in this example would result in a movement downward to a diagnostic display. Selection of Sector 0 would cause movement upward in all instances.

The sample hierarchy of Figure 4 will be used in the example of the next section and is introduced here to illustrate the form of a typical organization. The actual contents of each display are not necessary in establishing this structure; only the page names, numbers and a general idea of the purpose and function is required. The purpose and function of each display should be documented separately. A wealth of information is available in this figure, since paging and sectoring is already specified via the notations. The results of this first step may be likened to a functional description of the display system. The tree structure and philosophical descriptions of each page tell the user (operator) what the system will accomplish as he will see it. The details of each page are then provided in subsequent steps.

Output Description

Returning to Figure 1, the second step of the procedure identifies the display parameters necessary to accomplish the stated purpose of each page. This is a natural progression in detail from the philosophical description of step 1. Information at this point should specify the output variable name, the form in which the parameter is to be displayed (numerically, symbolically, etc.) and remarks concerning limits, alarm functioning and so forth. No information should be specified concerning display layout, since operations oriented personnel provide this input. The data should be gathered on a page-by-page basis to ensure continuity of display page documentation. This may require duplication of information if the same parameter appears

on a number of pages.

Input Identification

Once the output is defined, one must determine the source of this information. The plant instrument lists are the most logical reference for performing this task. However, this step does more than identify the parameter source. The data processing required to change the input to output is immediately implied and the methodology begins to involve computer oriented designers. Conversion to appropriate engineering units, off-set corrections and other needed manipulations become immediately obvious and must be accounted for in the computer pathway. Decisions may also be made at this time on the need for composed points where multiple instrument channels exist for the same parameter. A further, but important, advantage afforded by this step of the methodology is a cross check on the completeness of the instrument list.

Display Layout

The time has come to finally lay out each display as it will appear on the CRT screen. While a vague conception of the layout may have been necessary for guidance in the previous steps, it is best to start anew. Up to this point insufficient information existed to design the page intelligently. Display creation should be approached methodically, with sound human factors principles as a base. Too often the original concept used for guidance becomes cast in concrete without considering the details of the layout. The guidelines necessary for effective CRT display creation are discussed in Reference 3. Although a manual or semi-manual layout (such as a paper grid) may seem crude, it is really the only way to account for design details. Interchanger spacing, display density and loading, as well as other human factors, are difficult to account for without such a tool. Furthermore, the effort involved in laying out the display on paper provides more time to consider the details.

Processing Specification

The final step in the methodology is done by those intimately familiar with the display system, rather than the process being controlled. Decisions and specifications must be made concerning the real-time updating of the displayed data by the computer. Operations such as limit checking and alarming must be included to make the display useful. This step adds dynamics to an otherwise static picture and requires the appropriate expertise to make it come alive.

The end result of the procedure just described is a set of interrelated display pages designed to optimize the man-process

interface. A complete package of documentation is also a consequence of these steps. The package provides the necessary information on the overall organization of the display set and details on each page as it progressed through the design. An example that illustrates the establishment of a sample hierarchy and the effectiveness of the methodology follows.

ILLUSTRATIVE EXAMPLE

Consider a simplified NSSS as the system to be controlled. Major components of the primary loop include the pressurizer, two steam generators, four reactor coolant pumps, a chemical and volume control system (CVCS) and all interconnecting pipes. The task is to design a display set that meets the needs of the operator during normal and abnormal power operations. The logic involved in establishing the hierarchy for such a system will be discussed and the end results of the methodology demonstrated using sample displays. Since this discussion is only for illustration, there is no attempt to completely describe the display set. Additional pages are required for a realistic system which increases the number and complexity of the set.

The design starts by determining the needed displays and specifying their interrelationships. The most obvious display is one that presents an overall summary of the NSSS, showing major components. Each component or subsystem on this summary usually requires operator interaction, hence a display page will be allocated to the pressurizer, each coolant pump and CVCS. Although the steam generators are an integral part of the system, no operator interaction is provided on the primary side. Therefore, the displays for interaction with the generators would be included in the set for the secondary (BOP) side. It is apparent that many parameters are measured that are only of infrequent interest to the operator. This does not imply that they are not important. They certainly are under certain conditions, but not continually. Such parameters will be relegated to detailed displays that treat only a portion of each component. Restricting the discussion to only the coolant pumps, each pump may be conveniently divided into a motor section and a pump section. Displays are assigned to treat each of these sections for each pump. To randomly access these displays, a directory is needed to relate page numbers and names. A summary of alarm messages is also desirable to consolidate alarms for easy access and action.

Figure 4 shows the organization of such a display set. The overall summary of the system is found on page 101, the NSSS Monitor, the directory (100) and alarm summary (102) are also placed at the moni-

tor level. The controlling displays for each subsystem are beneath the NSSS monitor. The control displays for the pressurizer and the CVCS are excluded from this figure for simplicity. Detailed information on each coolant pump is found on the diagnostic level. This structure treats progressively greater details as one goes from the monitor level, down through the control to the diagnostic level. It satisfies the requirement for logical organization and emphasizes the interrelatedness of the displays in all directions.

One can also see how paging and sectoring are implemented early in the design process. The numbers at the top of each display box represent the page numbers and indicate the displays obtainable using the forward/back functions. Paging forward from 202 will display page 203, while paging back displays 201. A circular list for sequential retrieval is also included in this scheme, allowing the operator to move horizontally along each level rapidly. Paging forward from 204 yields page 201, the start of the control level displays. Additionally, the vertical maneuverability is demonstrated by the sector numbers adjacent to the tie lines between sectorable displays. In all instances, choosing sector 0 will cause an upward movement to the next higher level.

Following the establishment of this hierarchy and the philosophical definition of the purpose and function of each display page, specific parameters must be identified. Each page has a data sheet that lists this information and is used to relate the output to the input. The display designer uses this data to create a detailed layout of each display and then passes it on for processing specification and implementation. Results of this implementation will now be presented to show the maneuverability afforded by the hierarchy. Actual CRT displays have been created for the shaded boxes of Figure 4 and will be used in the example.

Maneuvering through the hierarchy is accomplished using the Page Control Module (PCM) shown in Figure 5. To randomly access a display (paging), the operator presses the PAGE button, enters the three-digit page number and then presses EXECUTE. The selected display immediately appears on the CRT. Paging forward and back along a given level is done using the FORWARD and BACK buttons in the figure. Only one keystroke is required to accomplish this function. Sectoring is performed similar to paging. When the SECTOR button is depressed, the sector numbers appear next to the component on the display. The operator enters the one-digit sector number and presses EXECUTE to obtain the desired display from the next level.

Monitor displays typically contain informa-

mation necessary to assess operation and status of a system or subsystem. Parameters used in these displays must be carefully selected to reflect the operation of the entire system being addressed. The recommendations of Reference 3 state that representational and graphical methods of presentation are best suited for monitor displays. However, there are exceptions. A directory listing the available displays is functionally a monitor level display, but requires alphanumeric methods of presentation, as in Figure 6. The operator can select the desired page from this display and access it using the paging technique. The arrow in the lower right corner indicates that more information or overflow is continued on a back page and can be accessed using the FORWARD button. The back page, in this instance, would contain the list of available diagnostic displays. Back pages are not included in the hierarchy because their need is not apparent until the display layout phase. The continuation symbol is used only when a back page is required for overflow.

A more typical monitor level display using the representational method of presentation is shown in Figure 7. All parameters on this display have a great impact in the operation of the NSSS and concisely depict the functioning of this system. If sectoring is desired from this display, the operator presses the SECTOR button and the sector numbers (Figure 8) immediately appear next to the sectorable components. If one of these sectors is not selected within 30 seconds, the numbers are removed to maintain display cleanliness. Pressing SECTOR again will reinstate the numbers and allow sector selection as described.

Assume the operator selected sector 4, the controlling display for Reactor Coolant Pump 2A (RCP2A). He would then obtain the control display of Figure 9. Control displays aid the operator in his controlling task and should contain all the information needed for control. Parameters that must be observed during the controlling task should all appear on the same display, even though they may be parts of other systems. Operator procedures and guides for controlling the component are excellent sources for determining which parameters to display. This display is also sectorable to obtain either the motor or pump section of RCP2A.

Diagnostic displays contain all the instrumented parameters related to a portion of the component dealt with in the control display. Figure 10 shows the diagnostic display for the motor section of RCP2A. One expects a great amount of detail at this level and must use the alphanumeric method of presentation. Mimic diagrams are of little use when dealing with a large

amount of information on one display. If that amount is too great for one page, backpages may be used to contain the overflow, as discussed earlier.

Alarm indicators should be available at all display levels to help the operator find the offending parameter quickly and with no a priori knowledge of page numbers. These indicators complement the dedicated alarm list that specifies the problem parameter and where to find more information. If the operator is currently viewing a display that includes the offending parameter, that parameter is alarmed on the display and the operator can act directly. An alarm condition for pressurizer pressure is illustrated in Figure 11. An alarm message would also appear on the Alarm Summary display. If the offending parameter is contained on a page further down in the hierarchy, the operator must be so advised. This can be done by alarming an appropriate symbol on the display being viewed and turning on the sector number which would guide him to the display containing the alarmed parameter. At this point the operator may go directly to the desired page, as indicated by the alarm summary message, or negotiate the hierarchy to see if the alarm is causing disturbances in other portions of his system.

Assume the operator is currently viewing the NSSS monitor display, Figure 7, and excessive vibration occurs in the motor section of Reactor Coolant Pump 2A. Considering the hierarchy structure of Figure 4, he is currently viewing page 101 while the offending parameter is contained on page 305. The pump symbol for RCP2A on the monitor display of Figure 7 would flash in the appropriate alarm color and the number 4, the sector number, would appear next to it. The results of these additions are shown in Figure 12. If the operator chooses to follow the sectors rather than going directly, he presses SECTOR, 4 and EXECUTE on the Page Control Module to obtain the control display for that pump, page 203 (Figure 13). The motor section of this pump would also be flashing in the alarm color and have the sector number 1 adjacent. Once again he sectors and obtains the diagnostic display, page 305 (Figure 14), which has the offending parameter in alarm.

Thus, two simple actions by the operator bring him to the level he needs to diagnose the problem. Obviously, if the offending parameter is also contained on the control display, he need not perform the second step. This technique aids the operator in finding the source of a problem, but does not interfere with a different strategy he may feel is more appropriate. It does not force him to act in any way, but only advises him of a logical action.

Although this example is somewhat straightforward, a similar hierarchy must be established for each and every set of displays in the system. Furthermore, the sets must be tied together at the monitor level to ensure proper integration. The designer may often be faced with situations where control and diagnostic displays exist, but there is no associated monitor. This is certainly allowable and merely implies that the operator must page to the controlling display before using the sectoring method. Some monitor displays, such as directories and alarm lists, may not be sectorable. This is precisely the reason for performing this work early in the design process. The establishment of the hierarchy graphically portrays the display system and its interrelationships and permits easier design of the individual display pages.

CONCLUSION

The key element in designing successful advanced control systems is designing successful CRT displays to optimize the man-process interface. The operator maintains a mental model of the process he is controlling and uses the displayed information to modify his model for the given circumstances. The display system must be organized to complement the operator's schema and allow him to make the necessary observations quickly. The display design methodology just presented places great emphasis on the hierarchy and provides a means of creating the display pages within the hierarchy. A documentation package results that traces the design from conception to implementation in a concise and consistent manner.

REFERENCES

- (1) Human Factors Review of Nuclear Power Plant Control Room Design, EPRI NP-309-SY, Project 501, Nov. (1976).
- (2) Netland, K. and Lunde, J. E., "Experimental Operation of the Halden Reactor, Utilizing a Computer - and Colour Display-Based Control Room," Proc. of Specialist Meeting on Control Room Design, IEEE 75CH1065-Z, 12, July (1975).
- (3) Danchak, M. M., "CRT Displays for Power Plants," Instrumentation Technology, 29, October (1976).
- (4) Baum, A. S. and Drury, C. G., "Modeling the Human Process Controller," International Journal of Man-Machine Studies, 8, 1 (1976).
- (5) Neisser, U., Cognition and Reality, W. H. Freeman and Company (1976).
- (6) Sheridan, T. B. and Ferrell, W. R., Man-Machine Systems: Information, Control and Decision Models of Human Performance, MIT Press (1974).
- (7) Schweppe, F. C. and Mitter, S. K., "Hierarchical System Theory and Electric Power Systems," Real-Time Control of Electric Power Systems, E. Handschin (ed), Elsevier Publishing Company (1972).

ACKNOWLEDGMENT

Acknowledgment is made to J.G. Brooks, Combustion Engineering, for initial work in establishing the hierarchical levels.

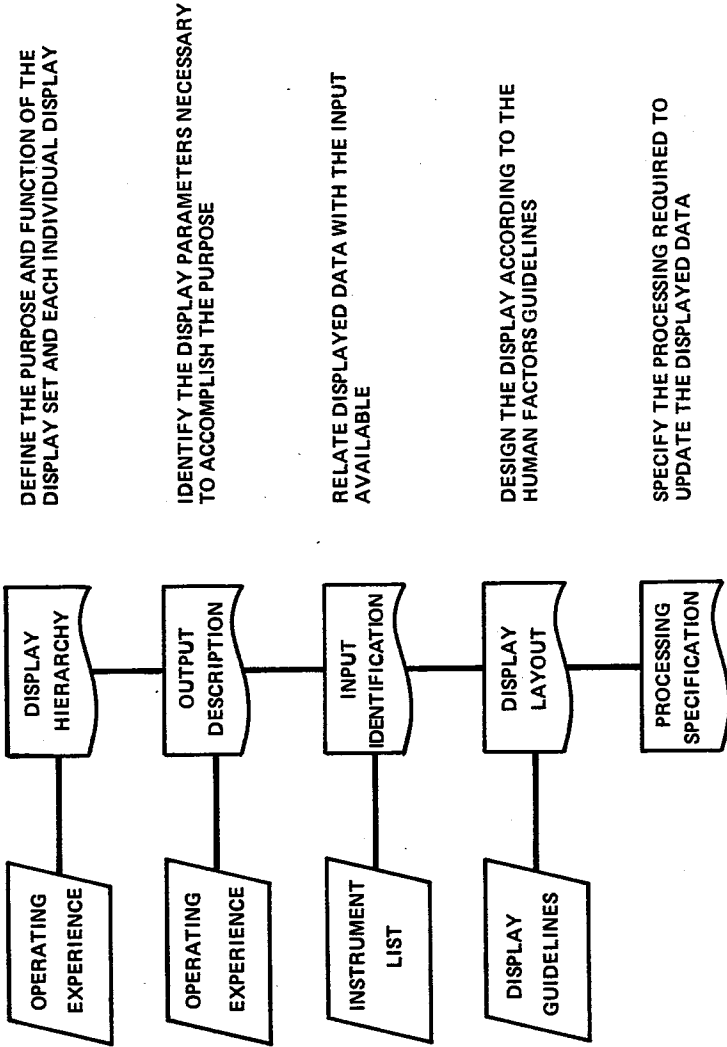


FIGURE 1. DISPLAY DESIGN METHODOLOGY

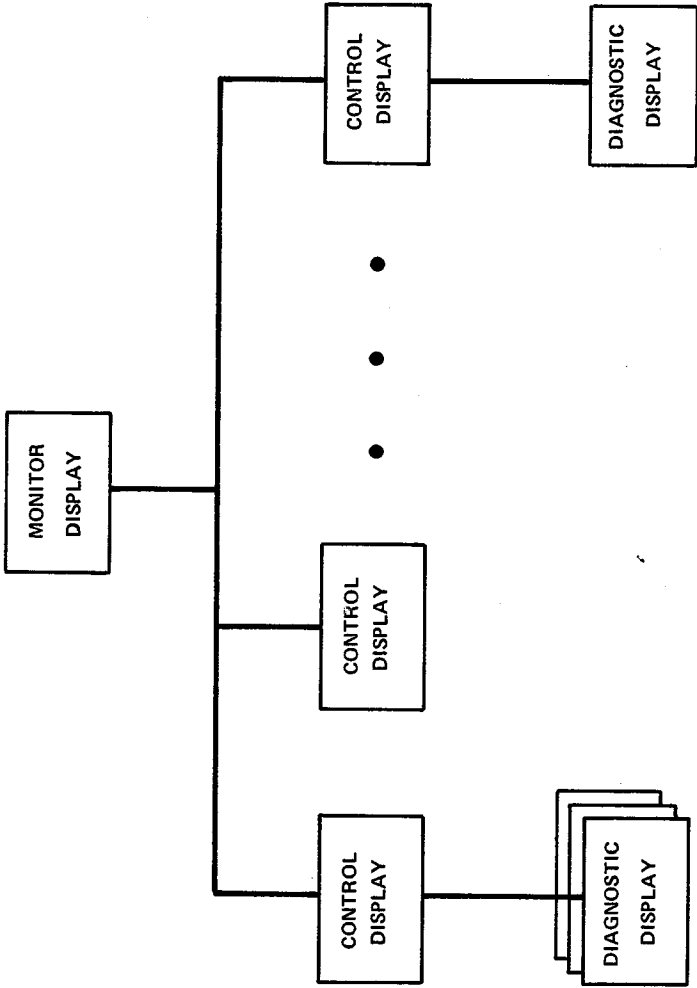


FIGURE 2. OPERATOR FUNCTION/DISPLAY HIERARCHY

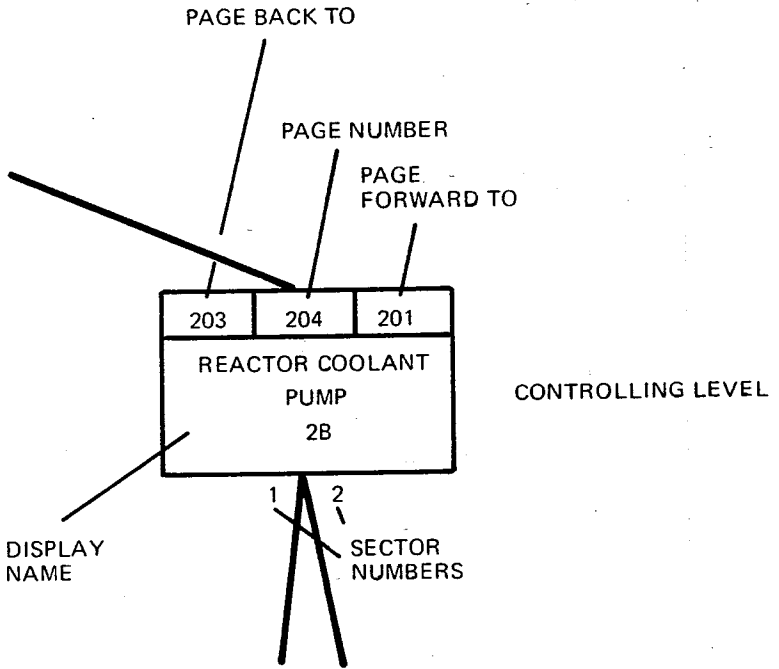


FIGURE 3. DISPLAY PAGE MANEUVERING INDICATORS

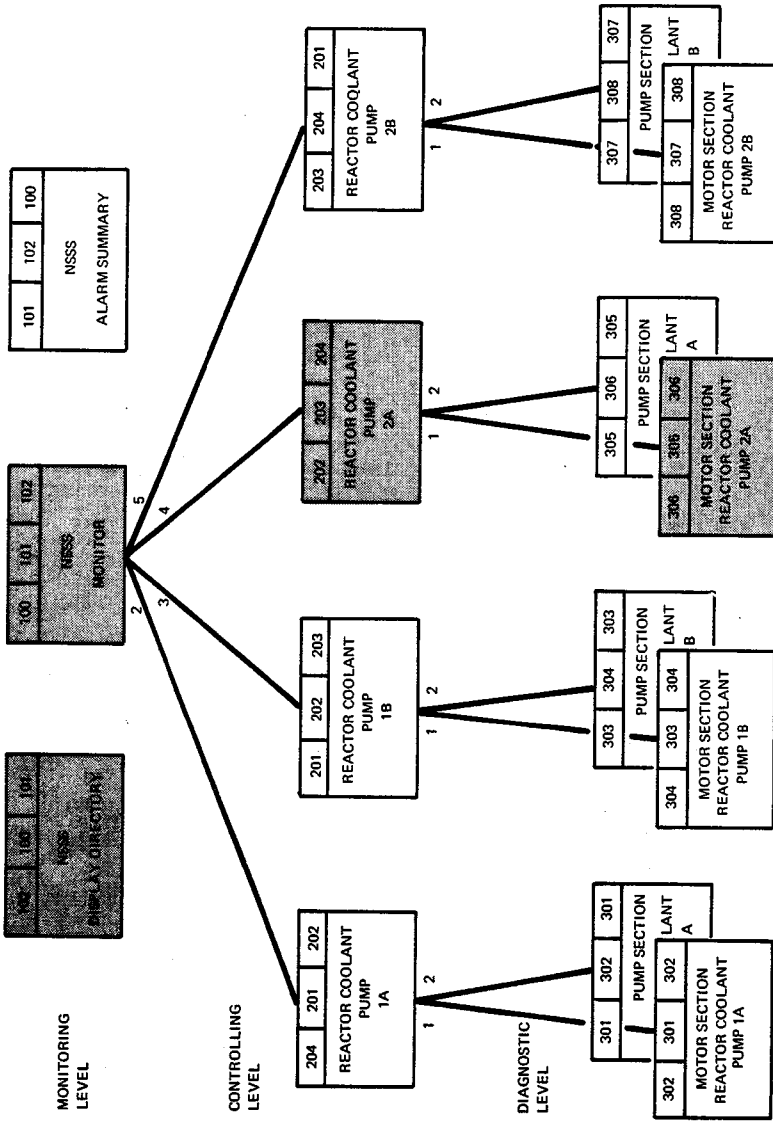


FIGURE 4. SAMPLE DISPLAY HIERARCHY

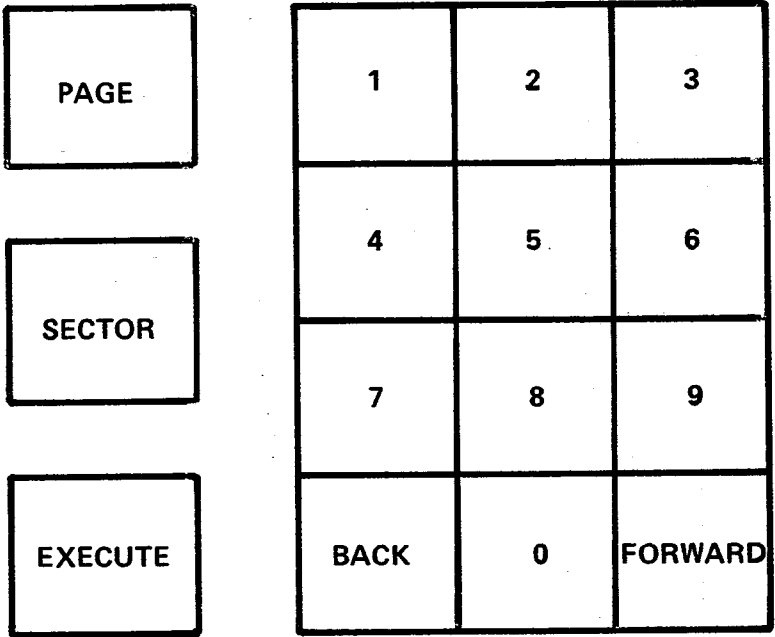


FIGURE 5. PAGE CONTROL MODULE

100
1013:05

100 - NSSS DISPLAY DIRECTORY
101 - MONITOR DISPLAY
102 - ALARM SUMMARY
(OTHER MONITOR DISPLAYS)

201 - RCP1A CONTROL DISPLAY
202 - RCP1B
203 - RCP2A
204 - RCP2B
(OTHER CONTROL DISPLAYS)

FIGURE 6. SAMPLE DIRECTORY DISPLAY



101
1813:10

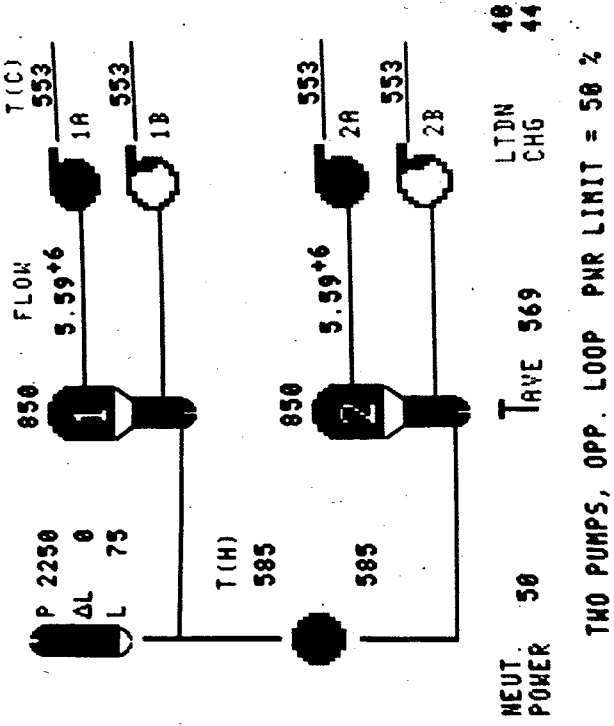


FIGURE 7. SAMPLE MONITOR DISPLAY

101
1813:10

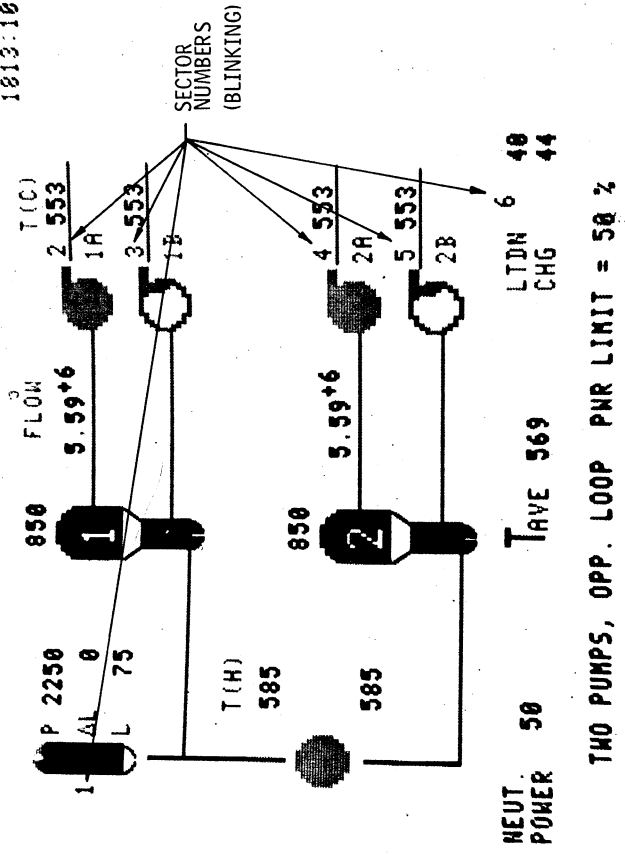


FIGURE 8. SAMPLE MONITOR DISPLAY WITH SECTOR NUMBERS

203
1013:15

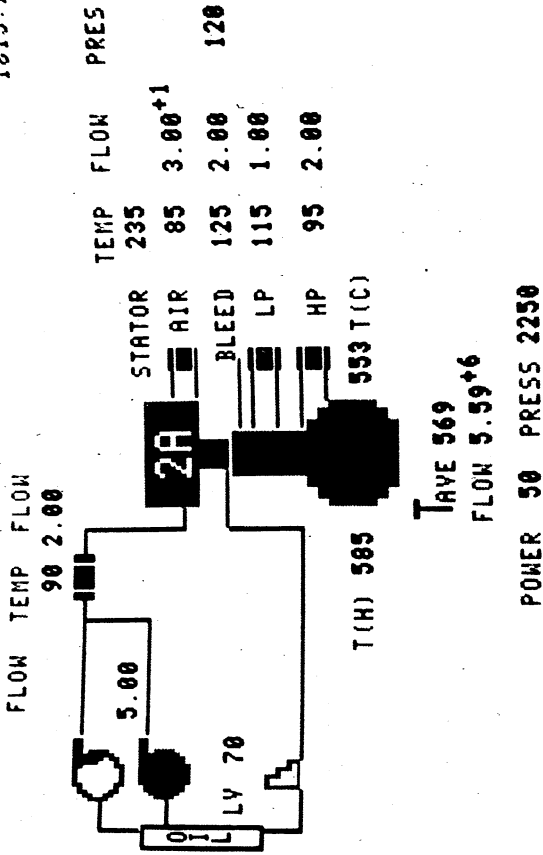


FIGURE 9. SAMPLE CONTROLLING DISPLAY

305
1813:20

MAIN OIL LINE	OIL	STRAINER	
TEMP 105	COOLERS		
FLOW 7.00	TEMP FLOW ΔP	2	
FLOW 7.00	885 2.00		MOTOR SPEED 860
PRES 10	885 2.00		VIBRATION .012
			TEMP
			BKSTOP OIL 130
			UP RAD BRG 135
			AXIAL BRG 140
			STATOR 220
			LW RAD BRG 147
			TEMP PRES
MAIN OIL TANK			UP JRN BRG 145
LEVEL 70			THRUST BRG 149
PRES 110			LW JRN BRG 150
OIL LIFT PUMP			
FLOW 5.00			
PRES 50			

FIGURE 10. SAMPLE DIAGNOSTIC DISPLAY

101
1813:10

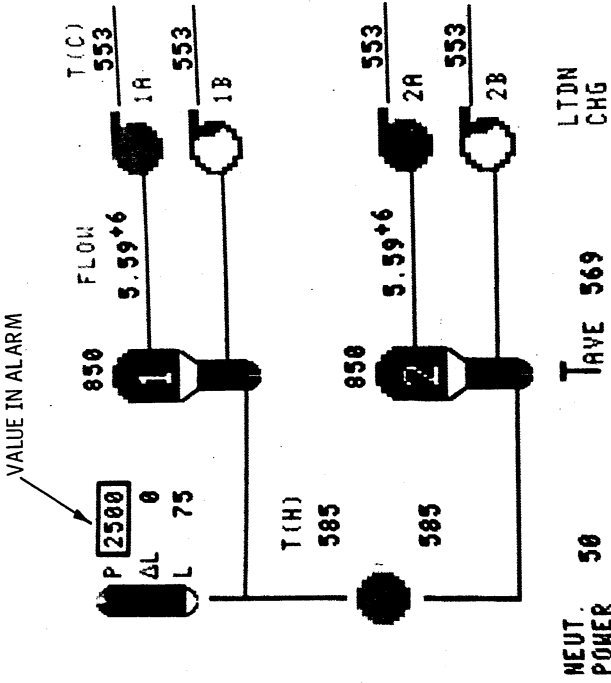
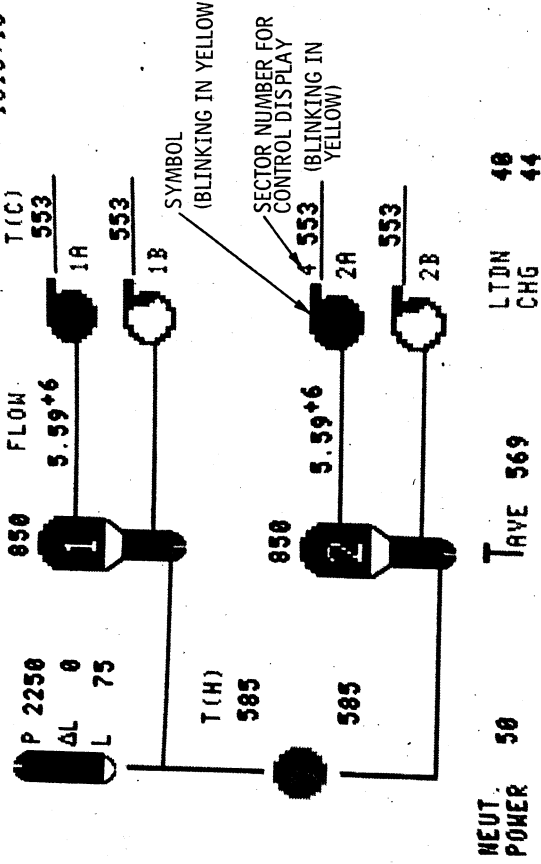


FIGURE 11. SAMPLE MONITOR DISPLAY WITH OFFENDING PARAMETER IN ALARM

101
1813:10



TWO PUMPS, OPP. LOOP PWR LIMIT = 50 %

FIGURE 12. SAMPLE MONITOR DISPLAY WITH INDICATION OF AN ALARM FURTHER DOWN IN THE HIERARCHY

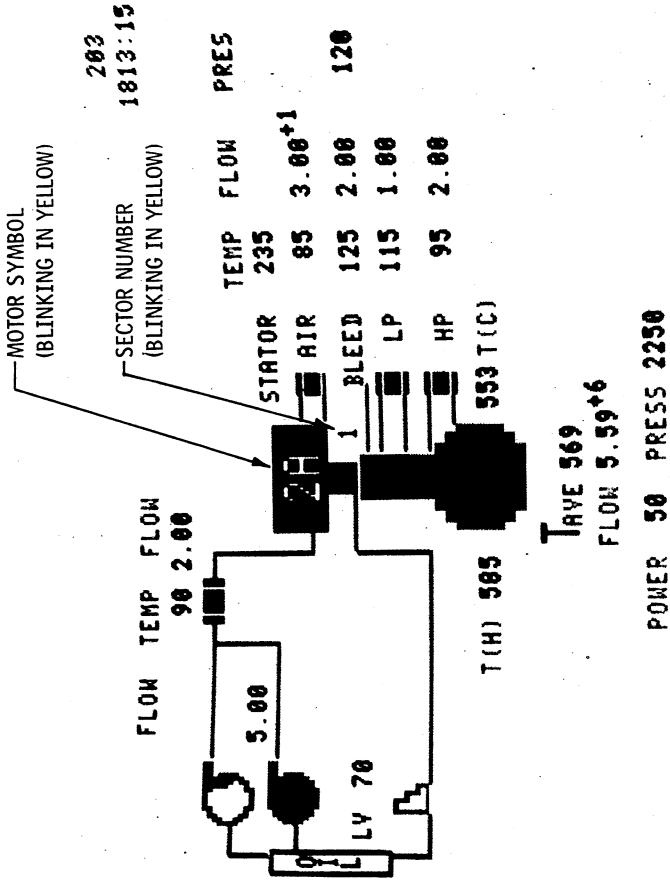


FIGURE 13. SAMPLE CONTROLLING DISPLAY WITH INDICATION OF AN ALARM FURTHER DOWN IN THE HIERARCHY

ALPHANUMERIC DISPLAYS FOR THE MAN-PROCESS INTERFACE

MICHAEL M. DANCHAK, Supervisor, Display Systems
Instrumentation and Controls Engineering
Nuclear Power Systems
Combustion Engineering, Inc.
Windsor, Connecticut

INTRODUCTION

As early as 1949, people working with computers recognized the shortcomings of printing devices for computer output and the potential of cathode ray tubes (CRT's) (1). The speed, bandwidth and flexibility of such a device is ideally suited for dynamic display of computer-generated information. Today the CRT is commonplace in computer terminals, vital to interactive graphics systems and is being used extensively for display of process control information. In the latter case, the CRT functions as the operator's window to the process being controlled (2). This device is rapidly replacing the myriad dials and meters to enhance operator comprehension and make his task more manageable.

Alphanumeric displays use alphabetic letters and numeric digits exclusively. They are a major subset of display systems that may include graphic and representational (mimic) pages (3). Color is also implemented in more sophisticated systems to add another dimension to improve operator awareness. Regardless of the level of sophistication, alphanumeric representation is the simplest and most common method of information display.

Unfortunately the display techniques used for printers are often carried over to CRT's, with little regard for the drastic change in display medium. This paper attempts to recognize that change and offers suggestions for the intelligent design of such computer output. The basic characteristics of CRT's are surveyed and the attributes of alphanumeric characters discussed from the human standpoint. The characters are then integrated to form display pages that satisfy the operator's need for information. Recommendations are made for creating the more traditional lists of alphanumeric information as well as the unusual layouts necessary for process control. All the recommendations are then summarized for easy reference and implementation.

CHARACTERISTICS OF CRT DISPLAYS

For the uninitiated, the technicalities of the transition from simple printed output to CRT displays is bewildering and frustrating. Terminology has been retained from the television industry, with some major exceptions. The rapid development of the computer-generated CRT display medium without accepted standard definitions and concepts, has resulted in display system vendors using the same terms to mean different things. A short primer on the characteristics of CRT displays is necessary to achieve some level of commonality for subsequent discussions.

A logical starting point for understanding is the cathode ray tube itself. At the risk of being trivial, basic concepts must be presented to appreciate the problems. Writing viewable information on the screen face is achieved by accelerating an electron beam and then deflecting it to impact that screen at the appropriate location. Here the electron's kinetic energy is converted to visible light by interaction with the phosphor coating. Deflection of the beam is related to an "address" generated by the display system. Since the emission of light from the phosphor decays with time, some mechanism is required to maintain the information on the screen. Storage tubes trace the data only once and depend on another source of electrons to preserve the data. In order to delete information, the entire screen must be cleared and the remainder

written again. Scanned tubes refresh the data by continually repeating the trace, using one of various scanning patterns. This requires the data to be held in some form of memory for refreshment, but erasing is done simply by deleting the unwanted information from this memory.

The size of the display area is a parameter that immediately causes confusion. As with the home TV, tube sizes are usually quoted in inches of diagonal; 17-inch, 19-inch and so on. English units of measurement will be used for illustration, since they are used by tube vendors and are more meaningful in this case. The CRT has evolved with a 3:4 ratio between the dimensions of the vertical and horizontal sides. Assuming a rectangle, this yields a nice 3:4:5 relationship between the vertical, horizontal and diagonal measurements, respectively. With a 19-inch screen, the sides should measure 11.4 and 15.2 inches. Unfortunately not all this area is available for display, since the tube is not truly rectangular. The parameter of concern, then, is the size of the largest complete rectangle that can be drawn on the tube. The nomogram in Figure 1

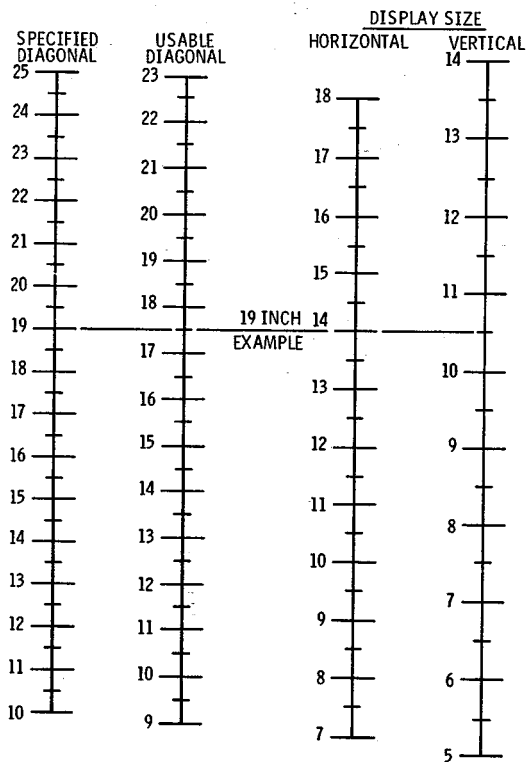


Fig. 1: CRT Display Dimension Nomogram

was devised to alleviate this problem, based on empirical data. One merely selects a specified diagonal and moves horizontally to obtain the dimensions of usable area. For a 19-inch monitor, the usable diagonal is 17.5 inches and the largest rectangle that can be drawn measures 10.5 inches vertically and 14 inches horizontally. These dimensions are extremely important in determining character size, as will be shown shortly.

Since various size CRT's can be used with the same display equipment, manufacturers work in resolution units related to the "address" mentioned previously. The screen is divided into addressable rectangles called pixels or picture elements, as shown in Figure 2. All patterns on the screen are built

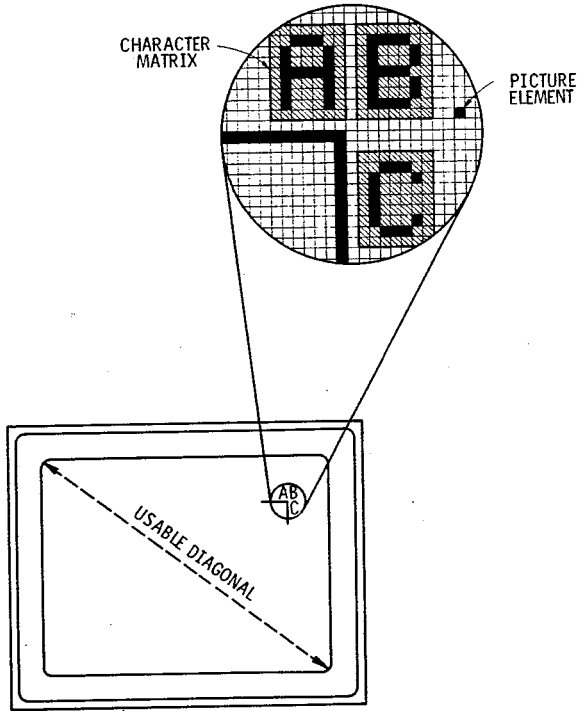


Fig. 2: CRT Addressability Levels

up using one or more of these pixels, whose measured size varies with screen size. Resolution of 256 x 256 (elements x lines) means there are 256 lines on the screen and each line is divided into 256 elements. A pixel may be placed at any one of 65,536 "addresses" resulting from the combination of 256 locations

along both the horizontal and vertical axes. For a 19-inch diagonal screen, each pixel would measure 0.055" x 0.0410" (width x height), or 0.050" x 0.037" for a 17-inch diagonal screen. Likewise, resolution of 320 elements x 240 lines (320 x 240) would yield pixels measuring 0.044" x 0.044" and 0.039" x 0.039" for 19-inch and 17-inch screens, respectively. The pixel size, and ultimately the character size, is predicated on screen size and resolution.

Figure 2 also illustrates another variable of character size: the character matrix. Alphanumeric characters are formed by a suitable arrangement of pixels. It would be extremely tedious to have to build each character every time one wanted to display that character. Therefore, character generators are included in display systems that function as character drawing subroutines. One specifies a starting location and a code to identify the individual character. The system then automatically forms the desired pattern according to a predefined matrix. In this instance, the matrix is composed of 63 pixels (7 x 9), but the actual character uses only 35 pixels (5 x 7). This is often written as a 5 x 7 character embedded in a 7 x 9 matrix; the excess pixels are used for spacing. This involves a critical distinction when computing character size. Using the 19-inch screen and 256 x 256 resolution, the character would measure 0.275" x 0.287".

A final characteristic of CRT displays is that of user addressability---the degree of positioning afforded the user through the host computer. Although the display system can address an individual pixel internally, such precision may not be available to the user. The terms "graphics systems" and "character oriented systems" will be used to distinguish the differences in addressability. Although "graphics systems" implies much more than addressability, its inherent capabilities allow the user to position the start of the character matrix at any pixel location. Thus, the user can vary the spacing and orientation between characters almost at will, as shown in Figure 2. "Character oriented systems" constrain the user to a much coarser grid called a screen matrix, Figure 3. Each element of the screen matrix coincides with a character matrix to form a number of character rows and columns. A "character oriented system" whose resolution is 420 x 405 and uses a 7 x 9 character matrix could display 45 lines of 60 characters each. The user may specify one of 60 locations in the horizontal direction and 45 locations in the vertical direction rather than the full 420 and 405. With this system, all spacing must be embedded in the character matrix unless blank characters are used.

With this brief survey one is better prepared to evaluate various systems and weigh the advantages and disadvantages of each. The discussions to follow do not account for such differences and rely on the reader to factor in this information when performing his own analysis. What can and cannot be done with a particular display system is a function of the tradeoffs made by the individual vendor and the market he is addressing.

ALPHANUMERIC CHARACTERS

In any discussion of alphanumeric (A/N) characters, one must be aware of the impact of character visibility, legibility and readability. Using the definitions of McCormick, (4) visibility is the quality of a character that makes it separately visible from its surroundings and treats the pixel level of detail. Legibility is the attribute of A/N characters that makes it possible for each character to be identifiable from others. Readability is the quality that makes possible the recognition of the information content of material when represented by A/N characters in meaningful groupings. Restating the definitions as a series of questions: Can you see it? What is it? and What does it mean? Since the pixel has been defined to satisfy visibility, this section will deal only with legibility by discussing the ideal character. The proper grouping of characters to form words and sentences is the ultimate goal and is treated in the next section.

Assuming adequate contrast and luminance, factors primarily dependent on hardware, one would like to specify an ideal character with which to compare available systems. The form of the character that allows the viewer to distinguish one from another is determined by character ratio, stroke width, matrix size, font, case and visual angle. Figure 4 illustrates these character attributes, their recommended values and representative variations. Character ratio refers to the relationship between the width and height and infers the squareness of the character. While the NAMEL(5) character set specifies a 1:1 ratio (square), reduction to 2:3 may be made without any appreciable attenuation in

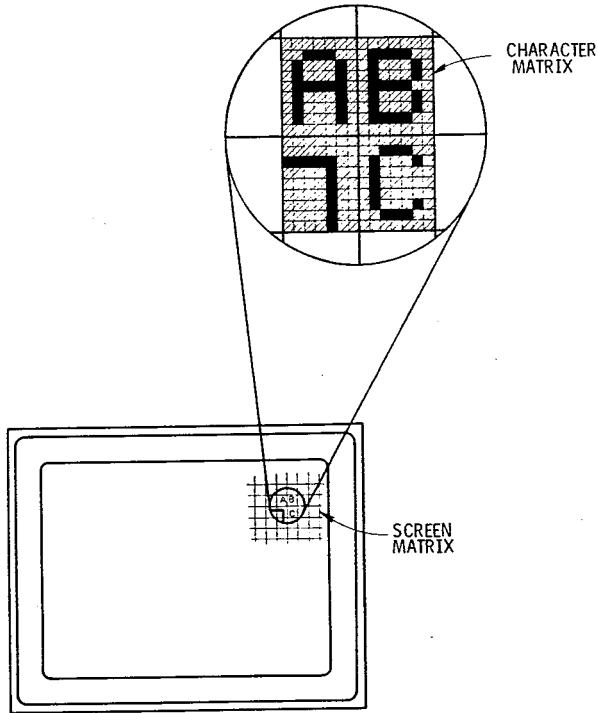


Fig. 3: Character Oriented Display System Addressability

legibility (4,6). The optimum ratio of the width of each stroke used to form a character to its overall height is given as 1:8 to 1:10(6,7). For self-luminous characters, as found on CRT's, the thinner stroke is preferable due to the phenomenon of irradiance (4). This accounts for the apparent increase in thickness of a line due to its brightness or contrast.

A minimum of 7 vertical matrix locations, or pixels, is required to represent most letters at a 90 percent recognition rate (6,7). A lesser number results in a significant decrease in legibility, while an increase to more than 10 achieves a corresponding increase in recognition to 95 percent. Given a 5 x 7 pixel matrix as a minimum, it has been found that fewer errors in character recognition result when a maximum number of pixels is used for the character outline (8). Such considerations are very important, since most vendors offer a user definable character set option that could be used to rectify deficiencies in the standard set.

Character case has an effect on both performance and preference. Studies indicate that upper case letters are more legible than lower case and are also favored by the viewer (9). Finally, to ensure legibility, the character height must subtend a minimum visual angle of 15-16 minutes of arc (6). The degree of

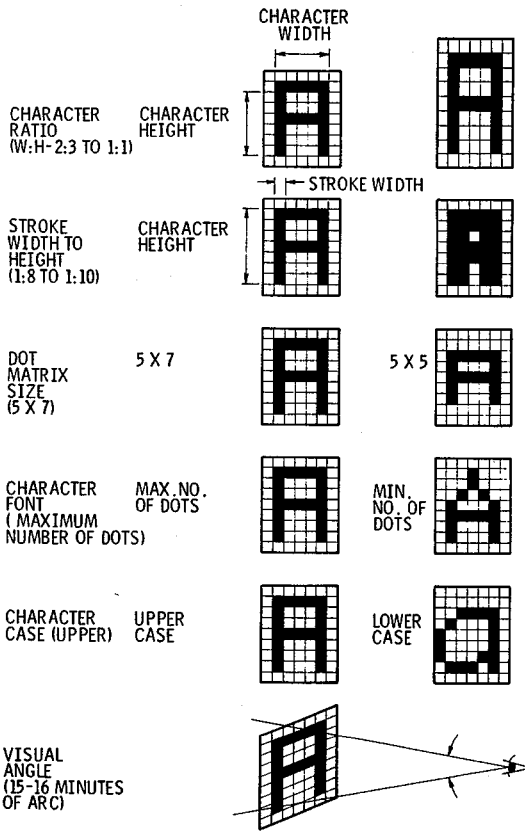


Fig. 4: Alphanumeric Character Attributes

subtension must be used as a unit of measure, since the viewing distance may vary for different applications. Conversion to actual character height will be discussed later.

One can immediately see that the pixel size has a great influence on the legibility of the individual character. The stacking and arrangement of pixels relative to one another determines all of the character attributes mentioned. While actual character forms will vary with system manufacturer, the ideal character described in Figure 4 will be assumed for the remainder of the discussion. Characters having these attributes will now be integrated into meaningful groups to produce readable alphanumeric displays.

ALPHANUMERIC DISPLAYS

Alphanumeric displays, by virtue of their purpose, tend to contain large quantities of information. It is the designer's task to simplify the display by giving the operator what he needs when he wants it. The designer must keep in mind that the operator learns and remembers, therefore, information about the steady state is often redundant⁽¹⁰⁾. While a certain degree of redundancy is necessary, the display must be optimized for change detection by the operator. Only by careful consideration of such human factors can the man-process interface be successful. The discussion of this category of displays will follow a list of questions formulated during prior work⁽³⁾. As shown in Table I, four major areas of concern must be addressed: format, coding, density and rate of change. Each area treats the alphanumeric display in progressively greater detail to produce a readable presentation.

Format

The format of alphanumeric displays deals with the overall organization of the presentation. Three questions must be answered before considering the individual elements that comprise the display: printed versus flow chart form, arrangement of information, and size of the display area. The majority of alphanumeric displays are lists of messages and/or parameters. However, a significant number may involve procedures or guidelines for the operator to follow in specific process control circumstances, such as startup or refueling. Generally it has been found that people misunderstand printed instructions one third of the time (the two-thirds comprehension rule). Under appropriate conditions, significant improvement in comprehension can be achieved using a flow chart scheme. By representing each step or decision in the instruction sequence as a separate process in the flow chart arrangement, operator comprehension can be increased to greater than 80 percent⁽¹¹⁾. Therefore, if the A/N display is used for guidelines or procedures, one should seriously consider organizing the steps in such a form.

TABLE I
GUIDING QUESTIONS FOR ALPHANUMERIC DISPLAYS

FORMAT	<ol style="list-style-type: none"> 1. PRINTED VERSUS FLOWCHART FORM 2. ARRANGEMENT OF INFORMATION CATEGORIES 3. SIZE OF ACTIVE DISPLAY AREA
CODING	<ol style="list-style-type: none"> 1. INDIVIDUAL VERSUS GENERIC LABELS 2. ESSENTIAL VERSUS NON-ESSENTIAL DATA 3. MULTIDIMENSIONAL CODING; COLOR, BLINK
DENSITY	<ol style="list-style-type: none"> 1. NUMBER OF DISTINCT INFORMATION CATEGORIES, PLACEMENT 2. NUMBER OF LETTERS AND DIGITS 3. CHARACTER SIZE AND SPACING 4. WORD AND SENTENCE SIZE
RATE OF CHANGE	<ol style="list-style-type: none"> 1. CHANGE OF DATA WITHIN CATEGORIES 2. CHANGE OF CATEGORIES

This point is illustrated by Figures 5 and 6. The example deals with a representative procedure the nuclear power plant operator must adhere to following a reactor trip. Figure 5 uses conventional printed instruction format to guide the operator through the critical steps. While this traditional representation is adequate, given a sufficient amount of time, there is serious potential for misunderstanding. Figure 6 may improve the comprehensibility of these procedures by using the flow chart concept. The boxes to the right of each branch signify the desirable condition, while the boxes to the left are abnormal and require operator intervention. Although multiple pages are necessary to present the same procedure, search and comprehension times for the entire procedure can be reduced.

If the content of the display is such that the flow chart technique is not applicable, one is still not constrained to using a purely columnar organization. The neat lineup of each row of alphanumeric data found in standard lists is valuable for comparison tasks, but adds to the confusion when information is not related. An implicit line is formed on the screen by eye motion as the operator scans a row of characters⁽¹²⁾. If additional but dissimilar data is placed on the same row, there is natural inclination to connect the two groupings. Intelligent rearrangement can avoid such implications and improve comprehension (Figure 7). While still labeled an alphanumeric display, the information categories are arranged functionally. Information categories are defined as one or more related parameters grouped together. The path from the Oil Lift Pump information category (comprising the related flow and pressure) to the Main Oil Tank category (level and pressure) implies a functional relationship between categories but not between the constituent parameters. Spacing and offset tends to interrupt eye movement to negate any implication of interconnection across the screen.

- * ALL CEA'S FULLY INSERTED? (MAN TRIP IF NOT)
- * REACTOR POWER DECREASING?
- * TURB TRIPPED & GEN BKR OPEN? (MAN TRIP IF NOT)
- * STM GEN PRES AT 900 PSIA?
- * FDWTR FLOW REDUCED TO 5% FULL LOAD FLOW?
- * (HI PRES TRIP ONLY) PZR PNR OPERATED RELIEF VLV OPEN?
- * (LO STM GEN PRES ONLY) MS ISO VLV SHUT?
- * (HI CNTNMT PRES/LO PZR PRES ONLY) SAF INJ INITIATED?
- * (SIAS/4160V BUS UMD V) EMER DIESEL GEN STARTED?
- * TWO RCP OPERATING?
- * PROPER PZR LVL BEING MAINTAINED? (MAN CTRL IF NOT)
- * UNIT LOADS XFRD TO RESERVE STA SVC XFMR?

Fig. 5: Procedures in Traditional List Format

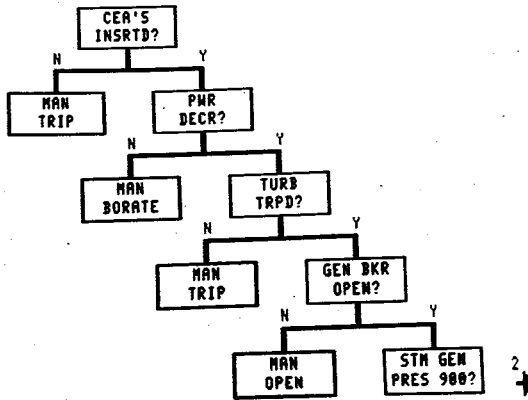


Fig. 6: Procedures in Flow Chart Format

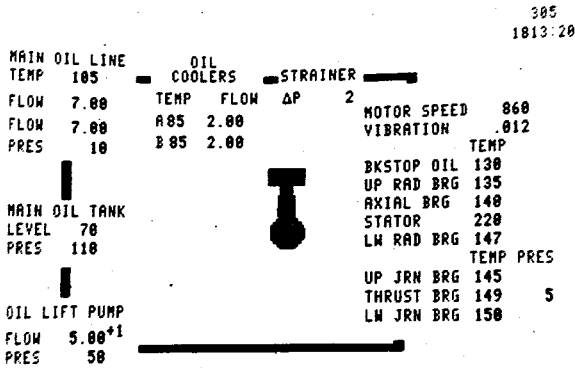


Fig. 7: Alphanumeric Display using Functional Format

When explicit lines on the screen are required, such as alarm lists and directories, each line forms its own information category as illustrated in Figure 5. In this case interconnection is not only desirable, but necessary to form the message string or sentence. Horizontal eye movement must be encouraged by using appropriate spacing between constituent words. Vertical movement must be discouraged by making the sentence a complete thought. More will be said on this when placement within information categories is discussed.

The third point involving alphanumeric displays is that of active display area. The usable display area has been defined in Figure 1. The question now arises as to how much of this area should be covered with information. Margins, forming "white space", have long been used in printed matter. But what constitutes a margin on a CRT? If one extrapolates from accepted charting techniques, an 11 percent margin should be allotted for the longer dimension and a 20 percent margin for the shorter side (13). Esthetics is another important, but often overlooked, consideration. Since the operator must view the same set of displays for an extended period of time, a pleasing display would also enhance comprehension. Although it is difficult to quantify esthetics, initial guidance may be obtained from the concept of the Golden Rectangle, which specified a ratio of 0.618034 between active display area borders. This relationship is a naturally occurring phenomenon and appears to be preferred by the majority of viewers(14).

Thus the active display area should be a Golden Rectangle that allows sufficient margin without violating the usable display area. A few simple computations yield a suitable rectangle that meets all of these criteria. As summarized in Table II, the specified diagonal was used to compute the tube size. The horizontal dimension was then reduced by 11 percent and the vertical dimension computed using the golden ratio. The results were rounded to the nearest half inch to define the active display area for representative systems. As seen in Table II, an active display area of 13.5" x 8.5" provides sufficient margin for a 19-inch screen, approximates a golden rectangle and still fits within the usable screen area. Naturally this is only a starting point and may be violated if layout circumstances dictate.

TABLE II
REPRESENTATIVE ACTIVE DISPLAY AREA SIZES

SPECIFIED DIAGONAL	COMPUTED SCREEN SIZE ¹ (X _m x Y _m)	USABLE SCREEN SIZE ²	ACTIVE DISPLAY AREA ³ (X _A x Y _A)
10"	8.0" x 6.0"	7.36" x 5.05"	7.0" x 4.5"
13"	10.4" x 7.8"	9.57" x 7.18"	9.0" x 5.5"
15"	12.0" x 9.0"	11.03" x 8.28"	10.5" x 6.5"
17"	13.6" x 10.2"	12.54" x 9.39"	12.0" x 7.5"
19"	15.2" x 11.4"	14.00" x 10.50"	13.5" x 8.5"

- $$X_m^2 + Y_m^2 = (\text{DIAGONAL})^2$$

$$X_m : Y_m = 4 : 3$$
- FROM FIGURE 1
- $$\left. \begin{aligned} X_A &= 0.89 X_m \\ Y_A &= 0.618 X_A \end{aligned} \right\} \begin{array}{l} \text{ROUNDED TO THE} \\ \text{NEAREST HALF INCH} \end{array}$$

Coding

Coding deals with the representation of information categories on the screen. For alphanumeric displays, the coding schemes are limited to characters and perhaps color, blink and intensity, if available. The designer's main concern is the effective portrayal of information using a minimum number of characters to increase comprehension and decrease density. Various techniques will be suggested that attempt to increase comprehension using the available coding schemes. These techniques will have a direct impact on display density.

One effective coding technique is the use of generic labels, whenever possible. This is particularly applicable within the context of information categories, as illustrated in Figure 7. The text string MAIN OIL TANK qualifies as a generic label for that category and has two sublabels, level and pressure. While the same information could be listed as MAIN OIL TANK LEVEL and MAIN OIL TANK PRESSURE, the increased density does not add information and therefore represents noise. Furthermore, the generic information category label tends to link the sublabels together, since the sublabels themselves are not sufficient for parameter definition. However, one must ensure that the generic label is readily distinguishable and that the sublabel relationship is obvious; e.g., through proximity.

Once the information categories have been defined, the display must be analyzed to place emphasis on the information, rather than the background. It is apparent that labels and sublabels are non-information bearing if they do not change their content during the life of the display. This criterion dictates that items such as dimensional units are also non-information bearing. Alphanumeric displays are the easiest to analyze for classification as to information content, provided one keeps the change criterion in mind. Parameter values that may vary qualify as information bearing; items that cannot change are background. This will be slightly modified in subsequent paragraphs to account for alarm conditions when color is available.

Color coding is another technique that can be very beneficial when used as a redundant code⁽³⁾. Given a seven-color plus black capability, each color must be assigned a specific purpose and used judiciously. Reference 3 details the considerations used in making this assignment and Table III lists the

TABLE III

RECOMMENDED COLOR CODES FOR ALPHANUMERIC DISPLAYS

<u>COLOR</u>	<u>USE</u>
BLACK	BACKGROUND
BLUE	LABELS, UNITS
CYAN	PARAMETER VALUES, OPERATOR MESSAGES
GREEN	STATUS WORDS (OF, CLSD)
WHITE	STATUS WORDS - INTERMEDIATE (ON, OPEN)
RED	STATUS WORDS (ON, OPEN)
YELLOW	CAUTIONARY ALARM
MAGENTA	ALARM - IMMEDIATE ATTENTION REQUIRED

standard colors and their associated conditions for alphanumeric displays. As stated above, items such as units and labels are non-information bearing and therefore are coded in blue, whereas parameter values use cyan. Since operator messages such as guidelines and directories are accessed for their content, they too should be coded in cyan. Black is used as the background color in all instances.

When the parameter value is a state rather than a numeric, the status word should be coded in either green or red to match the state. An alternative is to code the label in one of these colors and delete the status word entirely. However, this negates the redundancy desired for color and also puts unnecessary emphasis on certain components due to its label length. A valve whose label happens to be longer than others would attract more attention by virtue of length, which may not relate to its importance. The effects of such variations is minimized by using blue labels. Standard status words such as CLSD, OPEN, ON and OF ensure equal treatment and redundancy with a minor increase in density. When the state is intermediate to fully off and fully on (or closed and open), the status words ON or OPEN should be used with the white color. Additional information may be presented by using a lower intensity white to indicate that the component is currently being maneuvered within the intermediate state. A high intensity white would indicate that the component is currently fixed at some point between the state extremes. Adding another coding dimension, such as intensity, increases the information content without an attendant increase in density.

When a parameter on an alphanumeric display goes into the alarm state, one should change the color of both the parameter value and label to either yellow or magenta. This applies only to alphanumeric displays because of its density. Such a technique will greatly improve search and comprehension times. For a motor vibration alarm in Figure 7, the label VIBRATION and its value would be colored yellow so the operator can quickly differentiate which parameter is in alarm and its value. Labels at this time are information bearing. Another coding dimension can be added here by enclosing the alarmed value in a rectangle to reinforce the message. If the system also has a blink capability, it is best to blink only a small portion of the message, such as the rectangle or the value itself. Keep in mind, however, that it is difficult to read characters that blink between full intensity and off. Ideally one should remove the blink as soon as the search task is complete and before the operator actually processes the information.

An additional coding recommendation involves indication to the operator of continuation pages. Figure 6 rearranges the data of Figure 5 into flow chart format, but requires more than one display page to complete the presentation. The arrow in the lower right corner of Figure 6 indicates that more information on this subject is found on "the next page." A number is used to maintain operator orientation within a series of such pages (15). Thus the operator should be made aware of the continuation series and how far into the series he has gone with the current display.

Density

The next level of detail to be addressed in Table I is the density of individual information categories. Reference 3 determined that no more than 25 percent of the screen should be covered with data. The arrangement of constituent parameters and the number of characters used are important aspects in designing low density alphanumeric displays. The designer must determine the intended use of the parameter for each category. If a comparison task is intended for like parameters, the tabular arrangement is preferred. The operator can quickly compare digits without having to realize the actual values. The temperature and flow values for the two oil cooler loops of Figure 7 illustrate this point. The close proximity and columnar alignment of the two "85" numeric character strings tell the operator that both temperatures are equal. With a little more human processing, he may then realize that "85" is an acceptable value. Tabular arrangement also allows patterns to be detected between like parameters, as seen by the decreasing temperature sequence of the Upper Journal, Thrust, and Lower Journal Bearing entries of Figure 7. In all cases, parameter labels (or sublabels) should be left justified and parameter values right justified.

Since the columnar alignment is so applicable for comparison, one is immediately tempted to deliberately avoid such alignment for dissimilar

parameters within the information category. Returning again to Figure 7, why not stagger the constituent parameters to emphasize non-comparison of unlike parameters, such as the level and pressure for the main oil tank. Although this technique seems logical, it also destroys the orderliness of the display and makes it difficult to relate parameters to their information categories. In summary then, while it may be effective to avoid the tabular arrangement between information categories, it is best to use this arrangement for all constituent parameters within the category, regardless of their similarity.

Arrangement of the constituents within information categories of traditional alphanumeric displays is equally as important. While the format of Figure 5 may be improved using a flow chart format, the display as shown is a good example of a traditional representation and illustrates some interesting points. In this case, each line forms the individual information category, and the words that comprise each line are the constituents. As a minimum, one expects---perhaps erroneously---good sentence construction to dictate the placement of words. It is interesting to note that while syntax is precisely defined for computer input, little is said about the structure of computer output. Significant improvement in such output can be made by merely adhering to accepted grammatical principles and accounting for what is known as the serial position effect (16). This effect states that words at the beginning and end of message strings are more easily remembered (recalled) than the words between the extremes. Comprehension and retention of a message can be measurably increased by placing the most important words at these extremes. The lines in Figure 5 are concise and descriptive, containing little more than a subject and verb. Lines 6-9 state a particular condition and then an action. If the current situation does not match the stated condition, the operator need not read further. Similar techniques can be used to advantage on alarm lists, directories and other alphanumeric displays.

The next problem to be addressed in Table I is the number of letters and digits used within the information category. The numeric parameter value is read with best accuracy when there are four characters or less (3, 15). Since the status words have already been defined (ON, OF, OPEN, CLSD) to meet this criterion, the designer need only be concerned with numerics and labels. Values that contain only integers pose little problem in that the maximum (9999) is sufficiently large to account for most situations. Values having fractional portions do cause some concern and can be displayed in modified scientific notation. As illustrated by the oil lift pump flow value in Figure 7 (5.00 ± 1), the number of characters can be reduced without losing information by deleting the 10 multiplier of standard scientific notation. Although 6 characters are required, the representation is sufficiently compact so as not to cause unnecessary confusion. When the exponent of this notation is zero (i.e., the value is between 0.00 and 9.99), both the sign and the zero digit should be removed to aid the cleanliness of the display. Consideration should also be given to blanking values which read zero and leading zeros should always be suppressed.

Determining the number of characters for labels is not quite as simple due to the wide range of possibilities. Constituent parameter labels should always contain fewer characters, preferably 5 or less, than their associated information category label. Consistent and accepted abbreviations, such as PRES and TEMP, should also be used throughout, with all punctuation deleted (i.e., PRES versus PRES.) (15). The number of characters used for the category label should not exceed 12, but still must convey the information to the operator. Accepted abbreviations, mnemonics and acronyms consistent with the data base identifiers can be used to advantage in this case. If more than 12 characters are necessary, it is advisable to divide the string into smaller segments or "chunks" (17) using space characters, providing the label is amenable to such division. Punctuation should also be minimized in the message string (15).

Character size is another consideration in this display category. Figure 8 illustrates the relationship between character height and maximum recommended reading distance. The criterion for legibility is taken from Figure 4, which specifies a minimum visual angle of 16 minutes of arc. Since the character size in linear units is dependent on the display generator used and its associated pixel dimensions, the designer must perform a simple computation. Figure 8 then gives him the related reading distance. If the operator is expected to read a CRT message at a specified distance from the screen, the designer must use these relations to ensure such reading is possible.

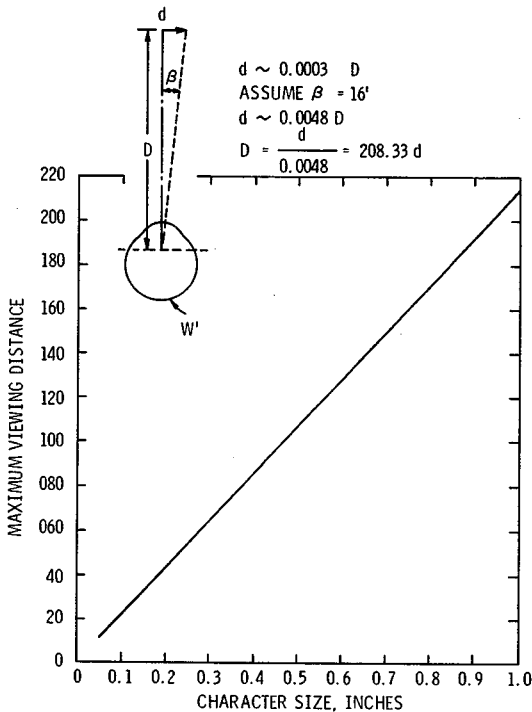


Fig. 8: Maximum reading distance for characters of various size

Spacing is an important element that has a large impact on the readability of alphanumeric message strings. The optimum intercharacter spacing is 75 percent of the character width(18). This results in a round off value of 4 pixels in the horizontal direction for the standard 5 x 7 character matrix. Care must be exercised in using this value, since the addressability constraints of a particular display system may not allow such spacing. Interline spacing is a function of the information category. Within the category, the lines should be more closely spaced to keep the data within the operator's span of attention. Quoted values of 30-50 percent of character height(6) for printed text are probably minimal for CRTs, due to the irradiance mentioned before. A value of 75 percent character height was chosen as the recommended interline spacing within information categories. For the 5 x 7-dot matrix, this translates to 5 pixels or 71 percent of character height achievable. Various intercharacter and interline spacings are shown in Figure 9. Blocks A, B and C have intercharacter spacings of 20 percent, 60 percent and 100 percent respectively while blocks D, E and F have respective interline spacings of 100 percent, 71 percent and 28 percent. Blocks B and E are identical, each having intercharacter spacings of 60 percent and interline spacings of 71 percent. These are the best approximations achievable with the display system used.

Sufficient space should be allotted between categories to avoid encroachment of one category on the span of attention of another. At 28 inches from a 19-inch CRT, the ideal distance between centers of adjacent information categories is 2 inches, representing a visual angle of 4 degrees. Here again, one must use this value as an initial guide for the display in question. If the display is a simple alphanumeric list such as a directory, vertical movement is constrained by having explicit lines. Hence, the interline spacing may adhere

A		B		C	
	TEMP		TEMP		TEMP
BKSTOP OIL	130	BKSTOP OIL	130	BKSTOP OIL	130
UP RAD BRG	135	UP RAD BRG	135	UP RAD BRG	135
AXIAL BRG	140	AXIAL BRG	140	AXIAL BRG	140
STATOR	220	STATOR	220	STATOR	220
LW RAD BRG	147	LW RAD BRG	147	LW RAD BRG	147

D		E		F	
	TEMP		TEMP		TEMP
BKSTOP OIL	130	BKSTOP OIL	130	BKSTOP OIL	130
UP RAD BRG	135	UP RAD BRG	135	UP RAD BRG	135
AXIAL BRG	140	AXIAL BRG	140	AXIAL BRG	140
STATOR	220	STATOR	220	STATOR	220
LW RAD BRG	147	LW RAD BRG	147	LW RAD BRG	147

Fig. 9: Variations in intercharacter and interline spacing

to the 75 percent rule unless a greater distance is desired for emphasis. At no time should the spacing be less than this amount.

Rate of Change

Rate of change determines how often the information on the CRT should be updated. In many instances the data base is modified at a very rapid rate. While the operator needs the most recent information, computer processing speeds are orders of magnitude greater than that of human processors. What does "most recent" mean to a human? The human "now" or psychological present is a time interval between 2.3 to 3.5 seconds(19). Hence, there is a point at which one can saturate the human capacity by presenting data more quickly than it can be comprehended.

On alphanumeric displays, saturation for a single parameter is reached when the digits appear to "wheel," i.e., change faster than the human can adequately comprehend each discrete reading. This is an increasingly familiar event, considering the proliferation of digital readouts in modern display systems. Another factor to consider is the potential conflict with blink rates as the values change. The display of rapidly changing values could cause the display to appear to blink if the update and blink rates are similar. To prevent both these events, an individual parameter update rate of 1 Hz or less is recommended. This allows sufficient human processing time between changes and still provides recent information, within the response time of the operator.

While this 1-Hz rate is applicable for single parameters, one must be concerned with the entire screen update as well. Each parameter update rate may meet the stated criterion, but appear on the screen at slightly different times to cause a twinkling effect which adds confusion. Assume the update rates of

parameters A, B, C and D are maintained at 1-Hz each, but sent from the computer with time separations of 250 msec. The operators' attention would be diverted from A to B to C to D, without allowing him to process each parameter. This twinkling can be alleviated by updating all the required parameters at the same time, no faster than once/second. This gives the operator a static picture of the process within the last second, much like the blink of an eye.

SUMMARY

Although alphanumeric CRT displays have been used to present computer-generated information for many years, the design of such displays has been left to the discretion of computer personnel with little guidance. It is the operator who must use this information. His attributes, rather than the computer's, must dictate the design. For the convenience of the display designer, the recommendations concerning alphanumeric displays are summarized as follows:

- determine pixel size and evaluate character attributes according to Figure 4
- consider the use of flow charts for procedures and guidelines
- avoid explicit or implicit lines when information is not related
- keep display density to less than 25 percent
- start with the Golden Rectangle
- use generic information category labels
- labels and units are non-information bearing; values are information bearing
- apply the color code of Table III
- number continuation pages
- avoid columnar arrangements between information categories unless comparison is desired; retain the columnar arrangement within categories regardless of the task
- left justify labels, right justify values
- account for the serial position effect
- use 4 digits or less to represent numerical values; use the modified scientific notation if fractions are necessary; suppress leading zeros
- information category labels should be limited to 12 characters; constituent labels should not exceed 5 and be less than the associated category label
- character size should be chosen to subtend 16 minutes of arc at the specified reading distance, Figure 8
- intercharacter spacing of 75 percent character width and interline spacing of 75 percent character height should be used within information categories
- 4 degrees viewing angle spacing should be maintained between adjacent information category centers
- update individual parameters no faster than once/second
- perform all required updates at the same time, within the one-second rate.

REFERENCES

1. Davis, S., Computer Data Displays, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1969.
2. Danchak, M. M., "The Man-Process Interface Using Computer Generated CRT Displays," Instrumentation in the Power Industry, Volume 20 (New Orleans, 1977), Instrument Society of America, Pittsburg, Pennsylvania, 1977.
3. Danchak, M. M., "CRT Displays for Power Plants," Instrumentation Technology, Vol. 23 (10), 1976, pp. 29-36.
4. McCormick, E. I., Human Factors Engineering, McGraw-Hill Book Company, New York, 1970.
5. United States Military Specification No. MIL-M-18012B (July 20, 1964).
6. Gould, J. D., "Visual Factors in the Design of Computer-Controlled CRT Displays," Human Factors, Vol. 10, 1968, pp. 359-376.
7. Sherr, S., Fundamentals of Display System Design, McGraw-Hill Book Company, New York, 1963.
8. Maddox, M. E., Burnette, J. T., and Gutmann, J. C., "Font Comparisons for 5 x 7 Dot Matrix Characters," Human Factors, Vol. 19, 1977, pp. 89-93.
9. Vartabedian, A. G., "The Effects of Letter Size, Case and Generation Method on CRT Display Search Time," Human Factors, Vol. 13, 1971, pp. 363-368.
10. Cornsweet, T. N., Visual Perception, Academic Press, New York, 1974.
11. Kammann, R., "The Comprehensibility of Printed Instructions and the Flow Chart Alternative," Human Factors, Vol. 17, 1975, pp. 183-191.
12. Green, E. E., "Message Design - Graphic Display Strategies for Instruction," Proceedings of the Annual Conference, ACM '76, 1976, pp. 144-148.
13. Enrick, N. L., Effective Graphic Communication, Auerback Publishers, Princeton, 1972.
14. Hoffer, W., "A Magic Ratio Recurs throughout Art and Nature," Smithsonian, Dec. 1975, p. 110.
15. Engel, S. E. and Granada, R. E., Guidelines for Man/Display Interfaces, Technical Report TR 00.2720, IBM Poughkeepsie Laboratory, Dec. 1975.
16. Murdock, B. B., Jr., "The Serial Position Effect of Free Recall," Journal of Experimental Psychology, Vol. 64, 1962, pp. 482-488.
17. Miller, G. A., "The Magic Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information," The Psychological Review, Vol. 63, 1965, pp. 81-97.
18. Hodge, D. C., "Legibility of Uniform-Strokewidth Alphabet; Relative Legibility of Upper and Lower Case Letters," Journal of Experimental Psychology, Vol. 1, 1962, pp. 34-46.
19. Miller, R. B., "Response Time in Man-Computer Conversational Transactions," Proc. of the Fall Joint Computer Conference, 1968, pp. 267-277.

DON FUQUA, FLA., CHAIRMAN

ROBERT A. ROG, N.J.
MIKE MCCORMACK, WASH.
GEORGE E. BROWN, JR., CALIF.
JAMES H. SCHRIER, N.Y.
RICHARD L. OTTINGER, N.Y.
TOM HARRIN, IOWA
JIM LLOYD, CALIF.
JEROME A. ANDRINO, N.Y.
MARILYN LLOYD BOGARD, TENN.
JAMES J. BLANCHARD, MICH.
DOMS WALGREN, PA.
FORNIE E. FLIPPIN, ALA.
DAN GLICKMAN, IARL.
ALBERT GORE, JR., TENN.
WES WATKINS, OKLA.
ROBERT A. YOUNG, MO.
RICHARD C. WHITE, TEX.
HAROLD L. VOLKMER, MD.
DONALD J. PEASE, OHIO
HOWARD WOLFE, MICH.
NICHOLAS HAYDOCKES, MASS.
BILL NELSON, FLA.
BERTL ANTHONY, JR., ARK.
STANLEY M. LUSHINE, N.Y.
ALLEN E. ERYTEL, PA.
KEAT HANCE, TEX.

JOHN W. WYCKER, N.Y.
LARRY WINN, JR., KANS.
BARRY M. GOLDWATER, JR., CALIF.
HARLTON FISH, JR., N.Y.
MANUEL LUJAN, JR., N. MEX.
HAROLD C. HOLLENBERG, N.J.
ROBERT K. DOORMAN, CALIF.
ROBERT S. WALKER, PA.
EDWIN S. FORSYTHE, N.J.
KEN KRAMER, COLO.
WILLIAM CARNEY, N.Y.
ROBERT W. DAVIS, MICH.
TORY ROTH, WIS.
DONALD LAWRENCE BITTER, PA.

COMMITTEE ON SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
SUITE 2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, D.C. 20515

JUN 07 1979

HAROLD A. GOULD
EXECUTIVE DIRECTOR

PHILIP B. YEAGER
NEOMA A. DAVIS
JAMES E. WILSON
WILLIAM D. WELLS, JR.
RALPH M. READ
JERRY STAUB
JAMES W. SPENELEY
STEPHEN LANES
IAN W. MARCEAU

MINORITY STAFF DIRECTOR
PAUL E. VANDER BRIDGE

Mr. Milton Levenson
Director, Nuclear Power Division
Electric Power Research Institute
3412 Hillview Avenue
P.O. Box 10412
Palo Alto, CA 94303

Dear Mr. Levenson:

Thank you for providing testimony at our subcommittee hearings on Nuclear Power Plant Safety on May 22, 1979. During these hearings you indicated that you would provide the subcommittee with responses to a number of questions, together with other additional information. Enclosed is a list of questions; we would appreciate receiving your response by June 25, 1979.

Thank you for your cooperation.

Sincerely,



MIKE MCCORMACK
Chairman, Subcommittee on
Energy Research and Production

Enclosure

SUBCOMMITTEE ON ENERGY RESEARCH AND PRODUCTION
HEARINGS ON NUCLEAR POWER PLANT SAFETY
ADDITIONAL QUESTIONS FOR MR. M. LEVENSON

1. Is there a need for a "Swat Team" composed of people from industry, the utilities, the NRC, etc.?
2. What are the advantages and disadvantages of standardizing the design of nuclear power plants?
3. What would be the attitude of equipment manufacturers and plant constructors to standardization?
4. Should there be a standard design for control rooms and for the layout of control room instrument and control panels?
5. Discuss and provide recommendations for means of using computers or microprocessors to enhance the power plant operator's ability to recognize abnormalities.
6. What design changes or procedural changes would you recommend to improve the defense against lesser accidents that you mentioned in your testimony?
7. What are your recommendations for improving the safety of nuclear power plants?
8. What role should your institution play in improving nuclear power plant safety?
9. List the research and development programs which you would recommend to improve nuclear power plant safety.
10. Should the training of nuclear power plant operators be improved? List your recommendations.
11. Should the control room operators be employed by the utility or should they be employed by some other agency?
12. How can the performance of the NRC be improved?