

JOHN O. PASTORE, R.I.
CHAIRMAN

RICHARD B. RUSSELL, GA.
CLINTON P. ANDERSON, N. MEX.
ALBERT GORE, TENN.
HENRY M. JACKSON, WASH.
BOURKE B. HICKENLOOPER, IOWA
GEORGE D. AIKEN, VT.
WALLACE F. BENNETT, UTAH
CARL T. CURTIS, NEBR.
JOHN T. CONWAY, EXECUTIVE DIRECTOR

CHET HOLIFIELD, CALIF.
VICE CHAIRMAN
MELVIN PRICE, ILL.
WAYNE N. ASPINALL, COLO.
THOMAS G. MORRIS, N. MEX.
JOHN YOUNG, TEX.
CRAIG HOSMER, CALIF.
WILLIAM H. BATES, MASS.
JOHN B. ANDERSON, ILL.
WILLIAM M. MCCULLOCH, OHIO

Congress of the United States

JOINT COMMITTEE ON ATOMIC ENERGY

October 11, 1967

DR-1433

Honorable Glenn T. Seaborg
Chairman
U.S. Atomic Energy Commission
Washington, D. C.

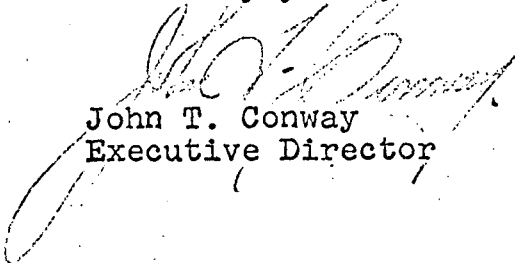
Dear Dr. Seaborg:

The Joint Committee has received the attached letter from Miss Elizabeth R. Hogan, one of the witnesses in the recent hearings on licensing and regulation of nuclear reactors. The Committee would appreciate receiving the Commission's comments on Miss Hogan's letter, particularly the questions she raises on page three.

In addition please provide the Committee with a narrative summary of the attempts by The Conservation Center to intervene in the Indian Point No. 2 reactor licensing proceeding; the official position of the AEC's regulatory staff relative to these attempts; and the pertinent rulings of the Atomic Safety and Licensing Board and of the Commission.

Thank you very much for your cooperation.

Sincerely yours,


John T. Conway
Executive Director

Attachment:
Ltr Hogan to Conway
9/22/67, w/attach.

8111200343 671218
PDR ADOCK 05000247
U PDR

Rec'd Off. Dir. of Reg.
Date 10/11/67
Time 2:55
Bath. 1

DR-1433

RECEIVED
SEP 25 9 41 AM '67
JOINT COMMITTEE ON
ATOMIC ENERGY

Benjamin Franklin Hotel
222 West 77th Street
New York, New York 10024

Sept. 22, 1967

Please initial and return to JSAC	
Chairman	
Vice Chairman	
Conway	
Bausser	
Burris	
Costagliola	
Dealingier	
Egan	
Kelso	
Low	
Miller	
Murphy	
Rodcliffe	
Tomen	

Mr. John T. Conway, Exec. Director
Joint Committee on Atomic Energy,
Room AE-1, U.S. Capitol Bldg.
Washington, D.C. 20510

Dear Mr. Conway:

It was indeed a pleasure to meet you, and a privilege to present my testimony before the Joint Committee. I was especially gratified by your suggestion that the Joint Committee review the Conservation Center's petition to intervene at Indian Point # 2, and Rep. Holifield's agreement to do so.

In reviewing my copy of this petition I'd like to call the Committee's attention particularly to the following objections contained in this petition:

#4 quotes the Safety Evaluation as stating: (with regard to Criterion 1 (b):

"Performance standards that will enable the facility to withstand without loss of the capability to protect the public, the additional forces imposed by the most severe earthquakes, flooding conditions, winds, ice, and other natural phenomena anticipated at the proposed site." (Page 16, Safety Evaluation of Indian Point 2)

The question then raised by the Conservation Center was: What about unanticipated natural phenomena ...?

Since this petition was submitted, at least two tornado watches have been issued for the New York City area. Fortunately, these tornadoes did not materialize. The question as to potential damage a tornado might cause to a nuclear reactor remains, however, and should be explored in the interest of public safety.

#9 quotes from Pages 37-38 of the Safety Evaluation as follows:

"Also of concern are the potential adverse effects of fires originating in the control and safety system wiring and/or within the control room itself. In our opinion, a direct, analytical safety analysis relating to the possibility of reactivity excursions resulting from such fires is, in practice, impossible due to the random nature of fire damage and the nearly infinite variety of possible circuit faults (some 'unsafe', some 'safe') which could result. ...

"In this connection, a literature search was conducted with the assistance of the computer facilities at the Nuclear Safety Information Center (NSIC) at Oak Ridge National Laboratory, to study the historical record of such excursions. NSIC has informed us that they were unable to find any records of incidents involving reactor damage as a result of fire-induced excursions."

The Safety Evaluation then continued: "Based on the foregoing considerations, we believe that Criterion 16 is satisfied."

The Conservation Center petition questions: "How can the AEC or the public be satisfied, when potential adverse effects of fires are admitted to be "of concern", when a safety analysis of them is impossible, and when there are no records of incidents involving reactor damage as a result of fire-induced excursions, on which to base proper safeguards?"

#18: The Conservation Center asked as its final question: "What system has been set up, and what system could suffice, to warn the public in the event of a major atomic plant accident at Indian Point II? The "highly improbable" blackout was self-evident. but how would the evacuation of people in the surrounding area of Indian Point II be effected, if this proves necessary?"

None of these questions were answered at the public hearings, (or to my knowledge, elsewhere), because the Conservation Center was not granted the right to raise them.

By citing these objections for special attention, I do not mean to suggest that the other objections raised in the Conservation Center's petition have been satisfactorily resolved. I think the Joint Committee will find that many of them deserve greater study, especially since the Indian Point 2 reactor will be located so close to millions of citizens.

To turn now from the Conservation Center's petition to the Initial Decision of the Atomic Safety and Licensing Board, issued October 3, 1966, directing the Division of Reactor Licensing to issue a provisional construction permit for Indian Point # 2.

This Initial Decision notes (Pages 10, 11) that "...ACRS has enumerated several items which they wish to review before the issuance of an unqualified approval for a construction permit. Specifically, their view is, in part, as follows:

"The Indian Point 2 plant is provided with two safety injection systems for flooding the core with borated water in the event of a pipe rupture in the primary system. The emergency core cooling systems are of particular importance, and the ACRS believes that an increase in the flow capacity of these systems is needed; improvements of other characteristics such as pump discharge pressure may be appropriate. The forces imposed on various structural members within the pressure vessel during blowdown in a loss-of-coolant accident should be reviewed to assure adequate design conservatism. The Committee believes that these matters can be resolved during construction of these facilities. However, it believes that the AEC Regulatory Staff and the Committee should review the final design of the emergency core cooling systems and the pertinent structural members within the pressure vessel, prior to irrevocable commitments relative to construction of these items."

Mr. John T. Conway

- 3 -

This Initial Decision also notes, (Page 12):

"These requests by ACRS ... reflect a concern not heretofore expressed in ACRS reports."

The comments by the Atomic Safety and Licensing Board on Page 13 of this Initial Decision are not reassuring, however, that the information requested by the ACRS will be provided at the time it has been requested, notably, in the ACRS' own words: "prior to irrevocable commitments relative to construction of these items."

The questions which occur to me are:

(1) When will the final design of the emergency core cooling system and the pertinent structural members within the pressure vessel be available for AEC, (and ACRS), review?

(2) Is Con-Edison absolutely obliged to submit these for review by the ACRS, "prior" to commitments for their construction?

I raise these questions because the comment of the Atomic Safety and Licensing Board on Page 13 of its Initial Decision states that: "...as a matter of practice, applicants for licenses to construct and operate nuclear facilities do keep the ACRS, as well as the Staff, informed respecting progress in design and technology for a facility even after the issuance of a construction permit. It is reasonable to conclude that the same informational procedures will remain in effect."

A final question is: Even though the Atomic Safety and Licensing Board indicates on Page 14 of its Initial Decision: "...there appears no doubt that the Commission will accede to this ACRS request." is there any real commitment on the part of the AEC to do so?

In reviewing the transcript of my oral testimony before the Joint Committee, I was sorry to find that my answer to Rep. Hosmer's question: "Can you point to any instances in this 21-year history where the AEC has given any evidence whatsoever that it would be under any condition pressured to neglect the safety of the public?" was inadequate.

At the moment the question was asked I did not think quickly enough, but I might have mentioned that the references made in footnote 5 of my supplementary material included the fact that the AEC had overruled the ACRS in granting a construction license for the Enrico Fermi plant. This action might have been cited in response to Congressman Hosmer's question, had I thought quickly enough.

Again, after careful study, I can think of no other way to interpret the examples given by Milton Shaw to inadequate workmanship and inspection in connection with AEC reactors, than the one which I gave in my testimony.

Mr. John T. Conway

- 4 -

In closing, I've found the pages of "The Technology of Nuclear Reactor Safety", Volume 1, edited by T. J. Thompson and J. G. Beckerley (copyright 1964 by M.I.T.), enclosed with this letter, helpful.

The Joint Committee may find them equally so, in considering the safety problems related to Indian Point nuclear plant # 2.

I don't know whether this letter and the enclosed material can be included in the record or not. If it can, it would be helpful in further explaining the concerns I expressed in appearing before the Joint Committee.

With thanks for your courtesy and attention, and again, for the privilege of appearing before the Committee,

Sincerely,

Elizabeth R. Hogan
Elizabeth R. Hogan

Enc: Pages 5, 6, 681, 682, 699, 701 "The Technology of Nuclear Reactor Safety" - volume 1, edited by T. J. Thompson and J. G. Beckerley, copyright 1964 by M.I.T.

2 page guide to significant data in AEC Authorizing Legislation-
Fiscal Year 1968, Part 2.

procedures is not considered within the scope of this project.

3 CREDIBILITY OF INDEPENDENT UNRELATED FAILURES

A reactor facility should be designed so that the failure of any single component will not immediately cause the failure of other components—that is, an arrangement like a “house of cards” should be avoided. For instance, if only a single electrical power source is available, its failure could cause loss of flow, loss of instrumentation power, loss of communications, etc. Clearly, all such failures must be designed against and prevented at all costs.

But what about independent or unrelated failures? Is it possible to experience accidents due to two or more independent events? Obviously, the probability of essentially simultaneous failures of two or more unrelated components is extremely small (see Sec. 1.4.3 of the chapter on Sensing and Control Instrumentation). However, the probability of two or more independent failures during any appreciable interval of time (i.e., seconds or longer) is not negligible.

The number of independent failures during a period of time deemed credible is a subject of controversy. Although everyone agrees that one failure can occur and can cause an accident, the credibility of two or more independent (and undetected) failures occurring in such a way and during such a time interval as to cause an accident has been debated. Some think it incredible that more than two such independent failures can occur. Others draw the line at a higher number.

A review of reactor accidents to date as carried out in the chapter on Accidents and Destructive Tests indicates rather clearly that often three or more independent causes for a reactor accident may exist. In our opinion three basic causes are involved in almost every reactor accident to date.

First, there is usually a design flaw—a hidden booby trap—which exists in the original reactor design and plays an important role in the subsequent accident. Elimination of design flaws is a most important function of a design team and of the safety review group. For example, the design of the SL-1 reactor required that each control rod be lifted by hand in order to attach it to the upper mechanism. At the same time, the design permitted sufficient reactivity control in a single rod so that the reactor could be made critical by withdrawal of this single rod.

Second, almost every accident involves a supervisor or human error of some sort. In the case of the SL-1 accident, the evidence is almost conclusive that the operators involved withdrew the central control rod far beyond the point called for by their orders. During the accident at Windscale, the supervisor, without aid of a properly annotated manual, made a command decision to reheat the reactor core, and this reheating basically was the trigger for the reactor fire.

The third parameter which is usually involved is some instrumentation problem. Included in the instrumentation problem is also lack of instrumentation. In both the SL-1 accident (no instrumentation operating except for one floor monitor)

and in the Windscale accident, instrumentation played an important role.

Thus, at least three causes exist in most accidents experienced to date. In some cases more than three causes have been involved and, in fact, in such a way that the elimination of any one of several causes would have changed the course of the accident materially or would have prevented it.

It is clear that the credibility of a number of independent failures must be taken seriously. Anyone who has read the story of the accident to the ship Andrea Doria or accounts of many other accidents will recognize that this is not a problem unique to nuclear reactors.

It must be emphasized that more than one failure can take place at essentially the same time if the failures are dependent—and the dependence may be very subtle. In fact, reactor designers and operators should beware of the label “independent.”

A structure as complex as a reactor and involving as many phenomena is likely to have relatively few completely independent components. Designers and operators must be continually alert to uncover relationships between potential or real malfunctions, and they must include consideration of reactor performance as a function of its life, since such an effect as misalignment or weakening due to wear (or corrosion or radiation distortion) can become an unrecognized common cause of a dangerous sequence of events.

In reactor facilities one of the chief booby traps exists because there are so many safeties involved. Some accidents have occurred because a relaxed or sloppy crew unknowingly has successively allowed various interlocks and safety measures to be breached one at a time; the logic of the operators always is that there are several and, therefore, the breaching of one is not important. Indeed, the results may be totally inconsequential until that time when the last in a long series is breached, and then the results may be very serious. This is one of the prime reasons why maintenance must ensure that all safety devices are operational at all times.*

4 NUCLEAR REACTOR SAFETY AND SAFETY IN OTHER INDUSTRIES

Except for the nuclear fission chain reaction and the associated nuclear radiations, the physical phenomena involved in reactor safety do not differ in any essential way from those normally associated with industrial plants. Industrial plants have hazards involving high pressures, high temperatures, potential chemical energy releases, corrosive and poisonous chemicals, fast moving mechanical parts, and so on.

Many industrial plants and storage and shipping facilities can, and sometimes do, experience energy releases far greater than even the worst ones which have been postulated as credible for nuclear reactors. Even the largest energy releases that have been estimated for hypothetical nuclear reactor accidents (which are believed to be well beyond the

*We exclude the built-in spare component from this discussion.

CONTRAST
 WITH
 "DECREASING
 PROBABILITY
 OF ACCIDENTS—
 AEC 1962
 REPORT TO
 THE PRESIDENT

realm of credibility) are relatively small compared to energy releases possible in certain industrial operations.

Because a nuclear fission chain reaction is the energy source, the reactor power level can increase under some conditions with extreme rapidity. Several chapters in these volumes are concerned with the kinetics of the chain reaction. As these chapters point out, there are ways to design a reactor so that the chain reaction is self-limiting. Even though basically complex, the chain reaction is controllable and proper reactor design can greatly reduce or eliminate the potential hazards associated with excessive energy generation in a "nuclear run-away."

The presence of nuclear radiations in reactors complicates the measures required to ensure safety. Remote operation of some components is necessary; this often involves mechanical complexity and a strong dependence on instrumentation. Means for maintaining those parts of the reactor that are, or may become, radioactive must be anticipated in the reactor design. Because a nuclear radiation field may preclude replacement of components, ruggedness and reliability are very important.

In spite of these considerations, for the most part the safety problems of nuclear reactor facilities differ only in degree from those of other industrial plants. The safe handling of radioactive materials requires the same kind of techniques and precautions as observed in handling dangerous chemicals or toxic biological substances. The design, construction, and operation of nuclear reactors require great care at all stages just as similar activities in other complex and potentially hazardous industries.

5 EFFECT OF ECONOMIC FACTORS ON SAFETY

As nuclear reactors develop into commercial sources of power, it has become evident that competition with fossil fuel plants is very keen indeed. In some geographic areas nuclear plants are now economically competitive with conventional plants. This has resulted in pressures on nuclear plant designers, constructors, and operators to reduce capital costs, to increase core life, to increase performance, to increase core size, and to reduce distances from metropolitan areas.

It is argued that the larger the plant the lower will be the capital costs per kilowatt of generated power. Experience to date indicates this.* There is therefore a substantial incentive to increase as rapidly as possible the size of plants and to extrapolate existing experience to much larger plants. This, of course, involves serious safety problems that are not easily answered. In particular, increasing the size of components, such as the reactor

vessel, valves, turbines, and so on, requires extrapolation of existing techniques and, consequently, some uncertainties result. Reactor physics may be somewhat different in larger, more loosely coupled cores with many more critical masses.

In an effort to reduce the capital costs, in particular those of transmission of electrical energy, considerable pressure has been exerted to move reactors closer to centers of use. The costs of rural transmission lines themselves range between \$50,000 and \$150,000 per mile, exclusive of right of way. Near urban centers where large quantities of electrical power are needed, the right of way is even more expensive and, in fact, in metropolitan areas, high voltage cables must be located underground. Such procedures are very expensive indeed and rapidly raise the costs of electricity. It is therefore clear that there are economic incentives to move reactors towards major centers of electrical energy consumption.

By increasing the performance of a given core, it is possible to improve the economics considerably. Almost every power reactor to date has been able to safely exceed its original design values and its power has been gradually raised. Increased core performance can be achieved by flattening the neutron flux distribution and thereby reducing the hot-channel factors. (The considerations involved in improving core performance are discussed in the chapter on The Reactor Core.) Pressures to increase core performance tend to force reactor designers to move closer to burnout conditions and to operate on narrower margins of safety as far as fuel is concerned. Thus, the burnout correlation and the validity of these correlations become very important indeed; the chapter on Heat Transfer emphasizes these aspects. As the flux is flattened, a larger and larger percentage of the core is being driven at or near the limiting thermal conditions. Thus, if there is a transient, fuel melting is likely to be more widespread than it would be in a reactor with a less flat flux.

As the safety margins are narrowed, it may be necessary to devise improved in-core instrumentation or to develop new means of burnout indication. To date efforts in this area have been limited; clearly, as performance has increased, such efforts become more and more necessary.

Another means of prolonging core life is by increasing the available reactivity. Since the total shutdown reactivity available in control rods in a power reactor is limited, it is necessary to limit the excess reactivity in such a way that the control rods can shut down the reactor in any conceivable situation. The only flexibility left is that which exists in core burnup or shutdown margin. Thus, the pressures to reduce the shutdown margin have been very great and in some cases the shutdown margin is now as low as 0.5% or less. This means that measurements of reactivity, reactivity effects, control rod worths, core lifetime effects, and so on, must be made much more carefully than formerly. At the moment, the state of the art in this area is not as good as it should be.

It should be noted that the incentives to prolong core life have also led to the design of new types of reactors which can be continuously fueled or refueled during operation on a partial basis. For

*For instance, the Yankee Atomic Electric Plant, operating at ~150 megawatts electrical, was built for approximately forty million dollars. The Connecticut Yankee Plant, operating at approximately three times this power level will only cost about twice as much. Experience is similar with boiling water reactors, such as those being built at Oyster Creek (New Jersey) and at Nine Mile Point (Oswego, New York).

and maintenance are followed, most of the problems of a disassembly after an accident will be minimized.*

(2) General Electric recommends high standards of cleanliness and good housekeeping as they had great difficulty with decontaminating and sorting out the equipment that was needlessly present.

(3) An emergency or alternative access to all areas should be provided.

(4) In areas where a high radiation operation could conceivably be carried out the crane should have all motions electrically powered and should have provisions for quick hookup of a remote or semiremote operating cable.

(5) Nonflammable building insulation should be used. The use of water cooling rather than oil cooling would also reduce the fire hazard.

Emergency Plans

(1) This accident again points out the need for clear emergency plans and adequate supplies. The first access was limited partially because no one other than the three operators knew what the situation was and no records from instrumentation existed and very few notes existed in the log. No radiation detectors with sufficient range were available at the site and no emergency supplies of health physics equipment.

Each reactor should establish one or more emergency depots remote from the reactor and clearly accessible. Each should have high level radiation detectors in operative order, self-contained breathing units, respirators, special clothing, up-to-date drawings as might be required in emergencies, and procedures for operations which might be necessary.

(2) The lack of an adequate written set of operating instructions and procedures seems to have played some part in the entire situation. Evidently, those available during the original startup and operation were deemed inadequate by the Office of Army Reactors, and more adequate ones were never prepared during the ensuing operations. It is clear that an adequate and up-to-date set of operating instructions, a set of standard procedures, and a set of check lists is vital to the safe and reliable operation of any device as complicated as a reactor.

General Concluding Note

As has been pointed out in the introductory chapter, most accidents involve design errors, instrumentation errors, and operator or supervisor errors. The SL-1 accident is an object lesson in all of these. There has been much

*It is interesting to note how strongly the General Electric group feels regarding these points. They were the ones who bore the brunt of the cleanup difficulties and it has clearly influenced their point of view. For instance, they had to remove and bury 15,000 ft³ (420 m³) of gravel used as vessel shielding and contaminated during the accident.

discussion of this accident, its causes, and its lessons, but little attention has been paid to the human aspects of its causes. There is a tendency to look only at what happened and to point out deficiencies in the system without understanding why they happen, why certain decisions were made as they were. Post-accident reviews should consider the situation and the pressures on personnel which existed before the accident. This section is presented to point out some of the factors which were involved in the decisions which were made. (It is hoped that others may take another path when they are faced with the same decisions and the same pressures.)

The design and operations attitude which permeated the project from its inception appears to have been more or less a direct result of the objectives set for the reactor, coupled with a limited budget, a tight time schedule, and constantly changing sets of personnel. The reactor was intended as "a prototype for the purposes of testing the operation and serving as a training center." [54] The requirements eventually developed called for 200 kw of electrical power with some expansion capacity and 400 kw of space heat. Because of the remote location and difficulties of refueling, it was desired that the core life be several years, and 3 years' equivalent was finally fixed upon as the goal. It was necessary that the reactor be capable of being operated by military personnel.

The original plan was to use nondevelopmental materials and fuel designs, but the long core life chosen and higher temperatures dictated the choice of X-8001 and a burnable poison. Pressures of schedule and developmental difficulties prevented putting the boron directly in the fuel element plates, and instead, side plates of partially clad boron-aluminum were chosen as being acceptable and providing more flexibility in selecting the final operating loading. (It must be remembered that nuclear calculations are often not too accurate on a new reactor concept. In fact, even rigidly specified duplicate cores on the same reactor may vary as much as 0.01 Δk in reactivity.) The flexibility was indeed used as discussed in reference [55]. No doubt the choice of the number and type of control rods was based on simplicity and ruggedness. The design clearly realized that there were some reactivity problems connected with the central rod. This rod had a much longer follower whose length appears to have been chosen to prevent a serious transient in the event the rod fell through the core and out the bottom. While the point cannot be easily checked and thus it is pure conjecture, it is possible that means were considered to make the assembly and disassembly safer and rejected on the basis of extra cost or, more likely, time schedule. The immediacy of a schedule delay or increased costs often outweighs the threat of a vague and improbable possibility. Other design errors were present and have been mentioned in the discussion. Most of these seem to point to choices dictated by the design objectives or made on the basis of cost and schedule limitations.

Once the design choices had been made, and the reactor built and tested, other factors

no doubt began to play a part. The initial tests seemed quite successful, giving everyone considerable confidence in the reactor. The design and startup groups, having completed their principal tasks, moved on to other work, sometimes not finding time to prepare adequate reports and operating instructions.

On relatively short notice, a new contractor took over responsibility for the plant. The transfer of responsibility for devices as complicated and individual as prototype reactors remains a difficult procedure at any stage, from initial design through to operation. It should only be done in cases of absolute necessity. Then it should be carried out over an extended period and in such a way that it is absolutely certain that all pertinent knowledge has also been transferred. It does not appear to this author that three months is an adequate period. Then too, the size of the staff which now took the responsibility appears to have been very small to carry out the many tasks assigned including becoming familiar with the reactor, preparing adequate operating instructions, training military personnel, and planning and supervising tests. Whether this was a budgetary choice or not is not known.

It should also be pointed out that the lines of responsibility for this particular project were especially confusing. The Department of Defense requested of the AEC that the reactor be built. The design, test, and initial operation was the responsibility of the Argonne National Laboratory. Pioneer Service and Engineering Company was the architect-engineer, and the Fegles Construction Company carried out the construction. The overall coordination and direction was the responsibility of the Programs Division of the AEC Chicago Operations Office. Later, the operation and in particular the Combustion Engineering part of the operation fell under the jurisdiction of the Idaho Operations Office of the AEC. The Division of Reactor Development of the AEC and its Army Reactors Office exercised over-all program responsibility. The AEC Idaho Operations Office and its Military Reactors Division, as well as the Army Reactors Office in Washington, participated in decisions regarding the amount of supervision to be used at the reactor. In testifying before the Joint Committee on Atomic Energy of Congress, C. A. Nelson, Chairman of the General Manager's Board of Investigation said, "The complexity of the chain of command for the SL-1 may explain, in part, the lack of effectiveness of the existing organization in communicating with higher levels of supervision regarding these substandard conditions." In the same hearing, Commissioner R. E. Wilson said, "The lines of responsibility within the AEC for health and safety, from the General Manager down to the operators of the reactors, were not clear and definite in several respects as they should have been, nor were the levels at which certain safety and operating decisions should be made spelled out."

While there were many people who, at least in principle, had some safety responsibility for varying periods of the reactor's life, no one or no single group exercised any continuous direct responsibility over all phases of its life. In fact,

it would appear that there was no one who was totally cognizant of the situation and at the same time had the authority, responsibility, and knowledge necessary to appreciate the problem and take decisive action. It is clear, and many people have later said so, that the reactor should have been shut down pending resolution of the boron difficulties and the general deterioration of the control rod operation. In fact, no one did so or even brought the malfunctions to the attention of any responsible safety group. In the climate that existed before the accident, it is likely that if one man had decided that the reactor should be shut down for safety reasons, he would have been ridiculed and would almost certainly have had an unfriendly response since he would have had to say some rather harsh things to accomplish his purpose.

The type of organization selected and its functioning has a fundamental role to play in reactor safety. The situation can be helped if four basic rules are adhered to as closely as possible:

(1) Insofar as possible, design, construction, and operation should all be the responsibility of one organization in order to ensure continuity and continued responsible judgment of the situation;

(2) The organizational responsibilities in regard to safety and all facets of operation should be clearly and unambiguously laid out. A line organization should be used, not a committee.

(3) Safety reviews should be made by a competent group outside of the operating organization on a regular basis. The safety organization should be such that these reviews are not repeated by competing safety groups so as to unduly harass the operating group and thereby reduce safety.

(4) The ultimate responsibility for reactor safety should rest and must always be allowed to rest on the immediate supervisory organization at the reactor. In the final analysis, the reactor shift supervisor and, in turn, the operator at the reactor console should have the authority to shut down the reactor if either believes it to be unsafe.

3.12 The SPERT-I Destructive Series [64-69]

General. During the summer and fall of 1962 a series of self-limiting power excursion tests were carried out at SPERT-I utilizing an 0.020 in. (0.51 mm) thick U-Al alloy plate-type element clad with 0.020 in. of aluminum. There were 25 elements in a 5 x 5 array in the core. There were one central transient rod and four other safety rods, each located in a separate quadrant. The double plate-type control rods operated in slots in special fuel elements. The water gaps between plates in the core were 0.179 in. (4.55 mm). This facility and core and the SPERT tests as a whole followed a logical development from BORAX-I tests described in Sec. 3.4.

A series of 54 tests were carried out using 5 core loadings, some of the later ones made up in part from undamaged fuel plates salvaged from earlier ones. The results for Cores II to V are summarized in Table 3-10 [65]. The tests showed plate buckling at periods of the order of 6 to 9 msec and a ripple pattern which would have led to heat transfer difficulties if the ele-

Table 6-1.
Causes of Accidents

Cause	Location (Date) Facility or Experiment
1. Personnel working in critical area (all fatalities)	LASL (21 Aug. '45, 21 May '46) Pu sphere; Vinca, Yugoslavia (15 Oct. '58) D ₂ O critical; LASL (30 Dec. '58) Pu soln.; NRTS (3 Jan. '61) SL-1; UNC (24 July '64) U soln.
2. Personnel working with non-safe fluid geometry	ORNL (16 Nov. '58) 55-gal. drum; LASL (30 Dec. '58) Pu soln.; NRTS (16 Oct. '59, 25 Jan. '61) fuel reprocess; Hanford (7 April '62) Pu soln.; UNC (24 July '64) U soln.
3. Loss of coolant*	Canada (12 Dec. '52) NRX; Hanford (4 Jan. '55) KW Reactor; Canada (July-Aug. '55) NRX; Canada (23 May '58) NRU; Santa Susana, California (13 July '59) SRE; Waltz Mill, Pa. (3 April '60) WTR
4. Loss of flow	ORNL (1948) X-10; NRTS (June '54) MTR; Hanford (4 Jan. '55) KW Reactor; Saclay, France (26 Nov. '57) EL-2; Saclay, France (13 April '58) EL-3; Saclay, France (12 Feb. '59) EL-2; NRTS (12 Dec. '61) ETR; NRTS (13 Nov. '62) MTR
5. Scram of control rods or control method causes accident	LASL (1 Feb. '51) critical; ORNL (1 Feb. '56) critical; LASL (3 July '56) Honeycomb; Vinca, Yugoslavia (15 Oct. '58) D ₂ O critical
6. Reactivity inserted too fast — source and startup	Hanford (16 Nov. '51) critical Pu soln.; LASL (3 Feb. '54) Godiva; Hanford (3 Oct. '54) production; Hanford (6 Jan. '55) production; LASL (3 July '56) Honeycomb
7. Positive feedback effects, an important factor	Canada (12 Dec. '52) NRX; Hanford (4 Oct. '54, 4 Jan. '55) production; Canada (July, Aug. '55) NRX; NRTS (29 Nov. '55) EBR-1; United Kingdom (9 Oct. '57) Windscale No. 1; Santa Susana, Calif. (13 July '59) SRE
8. Instruments caused accident	NRTS (18 Nov. '58) HTRE-3
9. Instruments off	LASL (Dec. '49) Water Boiler; Vinca, Yugoslavia (15 Oct. '58) D ₂ O critical; Saclay, France (15 March '60) Alizé; NRTS (3 Jan. '61) SL-1
10. Power decrease indicated, control rods withdrawn	Hanford (3 Oct. '54) production; NRTS (18 Nov. '58) HTRE-3; Waltz Mill, Pa. (3 April '60) WTR
11. Flat slab geometries or two units approaching	LASL (21 May '46) Pu hemispheres; LASL (1 Feb. '51) crit. cylinders; LASL (3 Feb. '54) Godiva; ORNL (1 Feb. '56) U ²³⁵ O ₂ F ₂ soln.; LASL (3 July '56) Honeycomb; LASL (30 Dec. '58) Pu soln.; ORNL (10 Nov. '61) critical
12. Experiment not well planned, parts performed unexpectedly	LASL (4 June '45) hand-stacked crit.; LASL (18 April '52) Jemima; ORNL (26 May '54) homog. crit.; NRTS (29 Nov. '55) EBR-1; LASL (12 Feb. '57) Godiva; UCRL (26 March '63) Kukla
13. Mis-estimates of effects of reactivity	LASL (11 Feb. '45) Dragon; LASL (18 April '52) Jemima; NRTS (22 July '54) BORAX-1; NRTS (29 Nov. '55) EBR-1; NRTS (5 Nov. '62) SPERT-1
14. Control rods withdrawn manually or by abnormal means	LASL (Dec. '49) Water Boiler; ANL (2 June '52) ZPR-1; Canada (12 Dec. '52) NRX; NRTS (3 Jan. '61) SL-1

* In NRX and WTR incidents, boiling caused loss of coolant and fuel melting. The SRE incident could also be categorized as a loss of flow accident.

primary cooling system unless subsequent over-pressure ruptures it.

In most reactors the accidents with the greatest potential for serious effects are those involving reactivity changes. This type of accident can occur while fission heat is already being generated in the fuel, or such heat may be generated because of the reactivity accident. This type of accident has the potential of utilizing all the forms of available energy to assist in dispersing the fission product burden of the core through the various containment barriers. Accidents involving reactivity changes do not have the advantage of being "sequential" in character.

To date nine cores have been destroyed or seriously damaged. Of these only two (BORAX-I and SPERT-1 Destructive Test) can be said to have been destroyed on purpose as a part of a test. Three reactors have been put out of action by accidents and never revived. Two of these, Windscale No. 1 and the SL-1, were deemed beyond reasonable repair. The third, Clementine, had really reached the end

of its useful life and was no longer believed to be a competitive research tool. It was dismantled and replaced by another higher flux research reactor—the OWR. These nine cases of core destruction all represent economic accidents of a serious nature involving radioactivity cleanup, down time, and rebuilding.

To date no accident has seriously involved the health and safety of the general public. The accident which came closest to doing this was the Windscale accident, which contaminated an area of about 200 square miles (52,000 hectares) around the reactor with a temporary low concentration of radioactive fall-out affecting the local milk supply. It cannot be said to have affected seriously the health and safety of the general public.

From the nuclear viewpoint and from the control viewpoint critical assembly and power reactor accidents have many similarities. Therefore, while recognizing that there are important differences, both of these types will be considered together in order to provide a larger number of accident

January 3, 1961, after a 10-day holiday shutdown. Enough others can be cited to indicate that judgment and alertness may be affected adversely on late shifts or on shifts where morale is likely to be low or where attention is wandering because of holidays or other reasons.

To date no serious accident has happened to any reactor which was operating at its normal operating conditions at its rated power. Almost all accidents have happened during startup or under special test conditions. In part, this may account for the large number of accidents just after holidays, since many reactors restart at such times.

6.2 Conclusions and Recommendations (See also those at the end of subsections on specific accidents.)*

(1) The single central goal of reactor safety is to prevent the release of fission products to the environment.

(2) Every reactor designer should strive to create a reactor system which is safe in spite of human errors, malice, or ingenuity. This implies that the system be designed as nearly fail safe as possible and that the core itself contain adequate inherent shutdown mechanisms such as voids, Doppler effect etc.

(3) All materials and components selected for use in reactor systems should have adequate safety margins on such parameters as tensile strength at operating temperatures, corrosion rates, compatibility, etc. No material used in any part important to the safety of the system should be used without a prior or concurrent and adequate testing program. In cases where such environmental tests are not deemed necessary, inspections at intervals frequent enough to ensure the integrity of the part should be carried out as a minimum. Quality control of all key components should be rigidly enforced during all stages of design, selection, and construction. Steps must be taken to be sure that the plant is built as designed and that all components continue to perform in accordance with the design objectives and specifications.

(4) Great care should be taken to utilize materials and fluids which are compatible from the chemical, corrosion, and structural viewpoints. Required materials which are not compatible should be separated by appropriate barriers.

(5) Accidents usually occur because of multiple and often apparently unrelated causes. It is not enough to place reliance on one simple safety barrier or procedure.

(6) Procedural control is at best a poor substitute for design ingenuity in setting up the first line of defense. That is to say, procedural controls should not be relied upon as the only, or even primary, safety barriers. Whenever possible interlocks and positive mechanical barriers should be

designed into the system to prevent unsafe actions. When such a system has been designed, procedural controls should then take over to ensure that the system is used and maintained correctly. In this sense, procedural controls also play a vital role. There is, of course, a point beyond which interlocks and barriers become so burdensome as to tempt operator ingenuity to violate them. This also has happened and should be avoided.

(7) Any solid configuration of fuel, absorber, or moderator should be so subdivided that the accidental or planned movement of any single piece will not cause an unacceptably large increase in reactivity.

(8) All possible mechanical movements and configurations in the core in both normal and conceivable abnormal conditions must be considered to see whether they are potential sources of large positive reactivity effects. In particular such movements should not increase the reactivity in an uncontrolled or rapid manner. The planned movement of any components within the core should be carried out so that only small portions of the core materials with safe incremental worths can be moved at one time and then only in a controlled manner.

(9) Those components of the system which control or strongly influence the insertion of reactivity into the system or the removal of reactivity from the system deserve particular attention in design, construction, and operation. The close coordination and mutual understanding of the reactor physicist, the metallurgist, and the mechanical designer are essential. The nuclear consequences of any normal reactor operation or any abnormality should be such as to be easily controllable by the available control systems.

(10) It should be impossible to withdraw by hand or other means in an unpremeditated manner control rods, the withdrawal of which could lead to criticality. This can be prevented by appropriate mechanical interlocks or by other design methods.

(11) In the United States it has become common practice to provide a shutdown margin sufficient to allow for the failure of a single control rod. This "Stuck-Rod Criterion" may be stated that it should be impossible for a reactor to be made critical in its most disadvantageous situation with only a single rod fully withdrawn. Consequently, it should always be possible to shut down a reactor with one rod stuck in its outermost position. If it is possible that rods or mechanisms might interact so that several could be stuck in the out position, the number of rods used in the Criterion should be increased accordingly.

(12) In Canada, Great Britain, and to some extent in the United States a "cocked-rod" rule is used. A control rod or rods should be cocked in the out position during all core changing operations ready to drop into the core in the event that a nuclear transient should result from any operation. In particular, the reactivity worth of the cocked rods should be greater than any conceivable amount of reactivity resulting from an accident during the planned operation. In some reactors such a rule is not possible and special care must be exercised during such operations as loading to ensure that the core is well below critical. (If the reactor

*The conclusions stated are those of the author of this chapter and do not necessarily represent those of the authors of the chapters on the various topics.

Guide to significant data contained in
AEC AUTHORIZING LEGISLATION-FISCAL YEAR 1968, Part 2*

(numbers which follow subject-heading indicate page numbers of this report)

Poor "quality" assurance; defects encountered in AEC reactor components:
Pages: 741, 784, 786, 1291-1292, 1297

Insufficient engineering standards; general rather than specific criteria:
Pages: 744, 757, 758, 1290, 1296, 1298

Instructions related to safety are not always written or followed: P. 743

Unsolved Technical and Safety Problems:

(Reactors are being built which require extrapolations on which technical data is not yet available, even though "major problems" are expected)

Pages: 698, 882, 883, 1407, 1418

Recent safety warnings: (From Advisory Committee on Reactor Safeguards)
Pages: 1327 to 1330

Nuclear reactor safety research is incomplete: (though large reactors are being built, and about to operate, without the advantage of the results of this research)
Pages: 902-903, 906, 1377 to 1382, 1407

Much that is known is not being applied; attitude of trying to "get by" when problems develop, without correcting the deficiency:
Pages: 742, 743, 776, 786

Severe Personnel Recruitment Problems: AEC and nuclear industry
Pages: 697, 769, 913

High-level radioactive wastes: Pages 855 to 858

Waste-tank failures have reduced storage space to "critical" status: P. 935-6

Inadequate industry expenditures for safety: Pages: 754-755

Reactor manufacturers balk at strict safety requirements: P. 763, 768, 1297-8;

Fuel used by nuclear power plants inferior to naval fuel: Page 769

Choice of materials related to safety is up to reactor manufacturers:
(inferior materials can affect safety but may be preferred because they are cheaper)
Pages: 769, 773 AEC does not inspect valves, etc. after fabrication: Page: 762

AEC will not force tested materials on nuclear industry: Pages 770-771

Self-regulation of nuclear industry (with regard to some inspections):
Pages: 786, 787, 788

AEC denial of full responsibility for public health and safety:
Conflicting statements, Page: 1287-1288

Dependence on individual worker's ability for reactor safety;
inability to get same degree of management attention (because of
numerous nuclear plants now being built) as before:
Page: 768

Inability to "place" responsibility:
Pages: 757, 788

Enrico Fermi meltdown accident, October 5, 1966: Pages: 778-779

Numerous technical-safety problems at Bonus reactor in Puerto Rico:
Pages: 922, 923

Explanation of barriers to fission-product escape: Page 1361

How accidents can lead to escape of radioactivity to environment:
Pages: 1365, 1368, 1369,

"Melting" can occur in less than a second: Pages: 1397 to 1399

Uncertain nuclear plant economics:
Pages: 745, 771

Operating History of Nuclear Power Reactors (through Dec. 31, 1966)
Pages: 1017-1073 (only shutdowns of five days or more are shown)

Updating of AEC 1966 Report to Congress: (Appendix 6)
Pages: 1074-1075
(Peach Bottom reactor shut-down three days after it started delivering
electricity to the Philadelphia Electric System: Page 1074)

Civilian Nuclear Electric Power Plants as of March 15, 1967: Page: 675

Nuclear Reactors built, Being built, or Planned in the U.S.: Page 993-998

AEC Report on Civilian Nuclear Power Program as of 3-31-67: Pages 1338-1339

AEC Budget for Fiscal Year 1968, Appendix 1: Pages 927-949

"Reactor Development Program.--Operating costs for the reactor
development program are estimated at \$492.3 million in 1968
compared with 1967 estimated costs of \$467.7 million and
1966 actual costs of \$428.6 million." (Page 930)

Admiral H. G. Rickover's advice to prospective purchasers of central
station nuclear power plants: Pages: 1493-1494

How many utilities have even heard of this advice?

How many follow Admiral Rickover's recommendations on safety assurance?

How well protected is the public in view of these admissions made
part of the record of hearings held March 14, 15, 1967 -- to
poor workmanship, defective, inferior materials; inadequate inspections,
unsolved technical and safety problems, lack of specific engineering
standards and criteria, conflicting data on "responsibility", etc. ?