INTERNATIONAL ATOMIC ENERGY AGENCY

INTERNATIONAL CONFERENCE ON CURRENT NUCLEAR POWER PLANT SAFETY ISSUES

Stockholm, 20–24 October 1980

IAEA-CN-39/ 6.4

NEW TRENDS IN SAFETY DESIGN AND ANALYSIS

D. OKRENT

University of California

School of Engineering and Applied Science

Los Angeles, California 90024

U.S.A.

Plenary Session VI of International Conference, October 20-24, 1980.
Paper Number IAEA-CN-39/6.4.

Abstract

NEW TRENDS IN SAFETY DESIGN AND ANALYSIS

The broad implications of the accident at Three Mile Island Unit 2 are examined for their likely effects on new directions and emphases in safety design and analysis. It is anticipated that a much more detailed and insightful understanding of plant and system behavior for a wide range of transient conditions, including small loss-of-coolant accidents, will be sought for use in plant design, in operator training, in the preparation of emergency procedures, and in efforts to develop disturbance analysis systems to help diagnose operational anomalies on-line and in real time. It is expected that greater attention will be given to undesirable effects which might arise from interactions between systems, and to the effect of control systems on safety. Improved shutdown heat removal systems, able to cope with a wide range of abnormal conditions, should also receive increased emphasis.

Potential inadequacies in the single failure criterion will be examined, both in terms of specific systems such as AC and DC power, and via a series of probabilistic studies of existing LWRs. The use of probabilistic methodology will grow very rapidly, particularly for determining possible weak spots in existing designs. A great need for quality assurance in probabilistic analysis exists.

Degraded core and core melt accidents will receive very considerable attention, both in analysis and design. It is recommended that design measures be implemented both to reduce the likelihood and to mitigate the

consequences of serious accidents, as proves practical and of significant benefit.

NEW TRENDS IN SAFETY DESIGN AND ANALYSIS

Major changes have occurred or may be in the offing with regard to safety design and analysis for light water reactors in the United States since the accident at Three Mile Island Unit 2 (TMI 2). The U.S. Nuclear Regulatory Commission (NRC) has required a large number of detailed changes as a direct outgrowth of the TMI 2 accident and is now considering some more general matters. In this paper, we shall examine several partly overlapping topics, some of which stem not from TMI 2 itself but from other recent operating experience or from general philosophic considerations of nuclear safety in the light of TMI 2. Most of these topics represent matters on which the U.S. Advisory Committee on Reactor Safeguards (ACRS) has made recommendations to the NRC. A brief summary of these recommendations is given in the appendix.

This paper is presented in the context of light water nuclear power reactors as they have been constructed and operated in the United States. All opinions expressed herein are those of the author.

The kinds of safety analysis and design change we will discuss herein can be crudely categorized into two groups:

- that which relates to trying to prevent an accident which leads to a degraded core or core melt.
- that which relates to the course of events during an accident involving serious core damage including core melt.

In what follows, we will discuss first the topics which are primarily analysis-oriented; however, a clear distinction between analysis and design

is neither possible nor desirable.

1. SMALL LOCAs AND COMPLEX TRANSIENTS

Analysis of plant behavior for a broad range of small-break loss-of-coolant accidents (LOCA) and complex transients has been given and will continue to be given greatly increased emphasis since TMI 2. The reasons for interest in such analyses are many, and include the following:

- Will the engineered safety systems meet their performance requirements, assuming they function in accordance with design?
- Can the plant recover from multiple failures both in safety and non-safety systems? Which, when and how?
- Will the operator have the information, knowledge and capability to cope properly with complex events and avoid aggravating them?
- How will the designers, regulators, and trainers of operators obtain a sufficiently detailed understanding of plant behavior?

Some examples of the many events of interest for such analysis are as follows:

- small break LOCAs anywhere in the primary system;
- small break LOCAs coupled with any of a wide range of complicating factors;
- two concurrent small LOCAs
- small LOCA concurrent with steam generator tube leak;
- small primary system LOCA coupled with loss of integrity of steam line or feedwater line;
- loss of offsite AC power coupled with a substantial steam generator tube leak rate and malfunction of other equipment;

- natural circulation heat removal under a wide range of complicating factors, including the need for boiling;
- feed and bleed, or bleed and feed cooling for extended periods of time;
- transients involving an over-supply of feedwater.

The requirements for accuracy, complexity, sophistication and speed of calculation will vary widely, depending on the application. Since essentially all these transients involve many minutes (or even hours) of real time, computing time may represent a significant problem, and there is likely to be a need to develop a new family of computer codes. A particularly challenging problem would be the development of a much more sophisticated simulator than that currently used for operator training, one which includes most all the control room functions and yet models system behavior physically and provides more detailed information on system behavior than is available from the sensors themselves.

2. SYSTEMS INTERACTIONS

Although the Advisory Committee on Reactor Safeguards (ACRS) identified the matter of systems interactions in 1974 [1] as one which had been treated inadequately and required much greater attention by designers and regulators, a relatively low priority was given to the subject by the NRC Staff prior to TMI 2. A classic example was the Quad Cities event in which failure of the non-safety grade, raw water system for the condenser flooded the turbine building basement in which pumps essential to shutdown heat removal were located [2]. Since TMI 2, the NRC Staff have given increased emphasis to systems interactions, and it is identified as a task in the action plan (3). The ACRS identified one practical approach to the matter in a letter to

Lee V. Gossick dated October 12, 1979 concerning the Indian Point reactors (4), and this approach has been pursued at the Diablo Canyon plant as part of an examination of the potential for earthquakes to cause undesirable systems interactions.

TMI itself raised some specific questions related to systems interactions, such as the adequacy of environmental qualification requirements for some equipment within containment and the auxiliary building. However, the general topic is expected to receive much broader attention.

3. DISTURBANCE ANALYSIS AND STATUS MONITORING

Methodology exists for status monitoring of components and has been applied in various degrees at nuclear power plants. What remains at issue is the extent to which it should be done on old or new plants. And, for some components suitable methods of instrumentation may require development. When the same components are used in a variety of different system lineups, the problem of status monitoring becomes somewhat more complicated but appears to be generally tractable. System and component surveillance during operation also appear to be tractable; however, the level of detail of surveillance becomes an important parameter, with tradeoffs to be expected between cost and complexity on the one hand and additional knowledge on the other.

Disturbance analysis systems (DAS) for on-line diagnosis of the causes and probable course of a transient (and to suggest possible courses of action to the operator) introduce an intriguing potential for long-term safety improvement which has received greatly increased interest since TMI 2. The previously on-going cooperative program between the groups in Germany and Norway has continued (5). This approach, which is fairly general and

ambitious in nature, initially has limited itself to monitoring feedwater and component cooling water systems. A disturbance analysis system will be tested at the Grafenrheinfeld nuclear plant as part of the regular operation of this nuclear station. The EPRI-funded program in the US, which had been aimed at developing a system which might improve plant reliability, has now been modified to have a safety orientation, and cooperatively with a new effort initiated by the Department of Energy, is trying to develop an approach to a Disturbance Analysis and Surveillance System (DASS) (6).

A super disturbance analysis and surveillance system, capable of on-line diagnosis of the causes and course of the very, very large number of different combinations of events which are of potential interest, is not likely to be practical, or perhaps even feasible. However, more limited although possibly complex applications of DAS or DASS may well develop. What may be of equal usefulness to the actual application of disturbance analysis systems to power plant operation is the deeper knowledge and insight concerning system behavior during a wide range of off-normal conditions, including those involving false information, which can come from the studies involved in attempting to develop a DAS, if this knowledge is applied in subsequent reactor design, in operator training, etc.

4. CONTROL SYSTEMS

In the past, the NRC has not reviewed control system design or imposed requirements on such systems except that they not cause failure of the safety systems supplied to protect against control system malfunction or other initiating events. The choice of control system design and the reliability built into the control systems were left to the reactor vendor and the designer of the balance of plant. Similarly, the NRC did not impose requirements on the reliability of instrumentation systems which provided information

to the control room except for that information which was designated as safety-related.

The Rancho Seco transient of March 20, 1978 began with failure of the power supply for much of the non-nuclear instrumentation. Erroneous signals were supplied both to the Integrated Control System and to the operator in the control room. The reactor underwent a fairly severe transient which included a loss of main feedwater, improper function of the auxiliary feedwater system, and actuation of the engineered safeguards. Proper information was not restored to the control room for seventy five minutes. (7).

The Rancho Seco transient was not ignored when it occurred; on the other hand, it did not receive an indepth evaluation by the NRC regulatory staff. Babcock and Wilcox recommended to its customers that limited steps be taken as a result of this transient; however, Babcock and Wilcox did not change the basic design of the non-nuclear instrumentation and its power supply.

After TMI 2, the Rancho Seco transient received further review. But it was not until the Oconee transient of November 10, 1979 and the Crystal River transient of February 26, 1980 (8), in each of which the operator again lost a large block of information during the very time the information was needed to recover from a transient associated with the same initiating event, that fairly major steps were recommended by the NRC and the Nuclear Safety Analysis Center (9) to improve the reliability of information to the operator against the same kind of failure. The ACRS had been suggesting and then recommending that the importance of "non-safety" systems, including control systems, to safety needed to be re-evaluated (10); however, this remained a relatively low priority item with the Regulatory Staff. In August, 1980

the ACRS recommended that the subject of control system reliability, including the reliability of control information to the operator, be declared an unresolved safety issue by the NRC (11).

Thus a deepening concern has developed that the past approach to control systems is inadequate for at least three major reasons. First, the design of control systems can have an important influence on the frequency and kind of transients that the safety systems will have to cope with. Secondly, the possibility that control system failure will not only cause a transient but hinder or negate the function of the safety systems needed to cope with the event has become more real (12). And, thirdly, the general question of the availability and accuracy of the control information normally supplied to the operator has become of concern (11). Hence, it appears likely that the proper design of control systems and the analysis of their role in safety will be areas of growing emphasis.

5. LOSS OF AC OR DC POWER

The loss of all AC power or DC power represents an event which goes beyond the single failure criterion and hence has not been normally the subject of safety analysis. The ACRS has expressed concern that neither of these two events had received adequate attention (13), and the NRC staff have relatively recently given priority to further evaluation of these issues, partly in response to the decision of the Atomic Safety and Licensing Board on the St. Lucie plant (14). However, experience at Millstone Point and Arkansas Nuclear Units 1 and 2, among others, should have provided a greater sense of urgency (15,16).

From the analysis point of view, it is of interest to understand plant behavior for a total loss of either AC or DC power for an extended

period of time, in order to provide insight for possible improvements in design and to help train operators and guide their actions in such an event.

Actually, the postulated events involving loss of AC or DC power should be taken as representative of a broader class of scenarios involving loss of redundant systems. Analysis should be made of the course and consequences of the loss of each important system for a wide range of events, whether due to a loss of redundant components or to multiple failures, in order to provide an improved basis for judging the potential and the need for improvement in design and/or operating training and procedures. The ACRS has been concerned with common cause failures for over a decade, and has reiterated its dissatisfaction with the single failure criterion several times since TMI 2 (10, 11).

6. THE USE OF PROBABILISTIC METHODOLOGY

Probabilistic methodology has become part of the LWR regulatory process and its use can be expected to grow markedly. The short term review of auxiliary feedwater systems by the NRC following TMI 2 and the resulting recommendations for increased reliability (17) were a harbinger of the future. The NRC staff has since initiated its Interim Reliability Evaluation Program (IREP) and the nuclear industry has separately begun reliability analyses of several specific plants (3). The ACRS had recommended such studies in its comments on WASH-1400 (18-20), and a similar recommendation was later made by the Risk Assessment Review Group (21). Nevertheless, it was TMI 2 that provided the spark for initiation of a substantive effect along this line. However, the NRC interim reliability evaluation program has moved relatively slowly, and in September, 1980 the ACRS reiterated its recommendation that the NRC adopt the earlier ACRS

recommendation that each licensee be asked concurrently to perform a probabilistic analysis of his own plant (22).

For plants in operation or under construction, the changes in design which will be practical are limited. It appears to be likely that probabilistic methodology will be applied to essentially all of these plants during the next several years in order to ascertain if there are any anomalously large contributors to risk and to provide a basis for judgment where significant improvements in reliability are practical and should be backfitted.

For plants to be designed, it is likely that probabilistic methodology will be used much more in design, as well as in safety review. The NRC is likely to impose requirements that go beyond the single failure criterion. Whether such changed requirements are deterministic, probabilistic, or a combination thereof remains to be seen.

In any event, the architect-engineer is likely to be forced into a new role. In the past, the balance of plant beyond that provided by the nuclear steam system suppliers was made to fit safety regulations, but little more, and frequently in a way that was too compartmentalized to have given proper appreciation to the significance of interactive effects or to common cause and miltiple failures. And relatively less regulatory evaluation was made of the adequacy of the balance of plant than of the nuclear steam supply system. This can be expected to change, and in the future the architect-engineer is likely to be heavily involved in probabilistic and other safety optimization of design.

The recent partial failure to scram at Browns Ferry Unit 3 (23) raises some serious questions concerning the way in which probabilistic methodology has been applied to reactor safety. The reliability of scram

systems had been an issue in connection with the matter of anticipated transients without scram (ATWS) for over a decade. The scram system was probably the system most studied using probabilistic techniques. The nuclear industry had argued vociferously that the system was far more reliable than the NRC staff and ACRS were willing to concede. The potential common mode failure via the scram discharge volume in a BWR had been known for a long time. (In WASH-1400 it was recognized but dismissed, mistakenly, as a very low probability event.) But, only after the Browns Ferry 3 event did detailed examination uncover many serious deficiencies in the design of the discharge volume system of existing plants (24).

This occurrence must give pause to one's acceptance of any claim of high reliability for a particular system, based solely on probabilistic analysis, and it highlights the need for the development of rigorous quality assurance for probabilistic analyses which are to be used in nuclear safety. All significant assumptions should be clearly displayed. The uncertainties in the results should be carefully presented. The authors should systematically discuss potential errors, weak spots, or omissions in their own work which might significantly modify or even reverse their own conclusions. A mechanism for peer review should exist for all analyses, whether performed originally by the industry or the regulatory body.

The analysis of DC power reliability performed by the NRC staff in 1978 provides an excellent example of the need for peer review, even of work done by a regulatory group (25). In that report, the NRC staff concluded that DC power introduced negligible risk and its failure could be neglected. The ACRS disagreed and the NRC Regulatory staff now appears to be changing its position.

There probably should be a requirement that any probabilistic analyses to be used in the nuclear safety design and review process be attested to, if not directed by, the equivalent of an especially well-qualified professional engineer whose specialty is nuclear reliability and safety.

7. DESIGN ERRORS AND SYSTEM DEGRADATION

One of the very difficult matters to deal with in probabilistic analysis is design errors. System degradation arising in some unexpected way, such as the multiple, deep, full-circumference cracks experienced at the Duane Arnold plant (26), are also difficult to deal with.

Design errors have tended to receive less attention in the past for their effect on reactor safety than has been warranted. When the work by Hsieh (27) indicated that design errors could be an important detractor to the adequacy of seismic design, that hypothesis was being advanced without the benefit of any direct empirical confirmation. Rather, it was deduced from other kinds of design errors which had been uncovered. Hsieh's suppositions have been confirmed by subsequent events (28-30). However, an improved approach to the detection and minimization of design errors and to the incorporation of design errors and anomalous system degradation into risk evaluation remains to be developed and warrants attention.

8. SHUTDOWN HEAT REMOVAL

Concern about the need for reliable shutdown heat removal for a wide range of possible scenarios did not arise with TMI 2. The draft WASH-1400 report had pointed clearly in 1974 to the importance of reliable shutdown heat removal for a variety of transients. An ACRS member, J.C. Ebersole, had been trying to get a similar message to the NRC and the U.S. nuclear industry for many years prior to TMI 2. He was developing design

concepts for a dedicated, bunkered, shutdown heat removal system intended to cope with fires, sabotage, earthquakes, among other things, (31) prior to the Browns Ferry fire. The idea received very limited support in the U.S. prior to TMI 2, although it has been separately conceived, developed, and implemented in some other countries, and the NRC had identified it as a priority item in its report to the U.S. Congress on a research program to improve reactor safety (32). However, it was TMI 2 that led the NRC staff to begin to emphasize the importance of reliable shutdown heat removal. They found soon after TMI 2 that auxiliary feedwater systems were not safety systems on all operating reactors and that,where they were safety grade, there were still many potential weak points in their design (17).

The NRC staff has identified shutdown heat removal systems as an important long range problem in its action plan (3) and it has been given an additional priority by being identified as an unresolved safety issue (33). However, it is not clear that a really comprehensive effort with the necessary large commitment of men and resources from government and industry to get the job done expeditiously has been made in the U.S.

It may be that, with an evaluation of the complexity of coping with multiple failures in the currently used shutdown heat removal systems, coupled with the complications that can be raised by the wide range of possible failures of control systems and non-safety systems, especially during a fire or earthquake, the use of dedicated shutdown heat removal systems will be accelerated in the U.S. Much more specific design effort is needed in order to evaluate and choose a proper set of design criteria for such a system. In any event, it is anticipated this will be an active area of safety design and analysis.

9. DEGRADED CORE AND CORE MELT ACCIDENTS

The ACRS recommended research and development programs related to core melt accidents in 1966 (34) and has reiterated this recommendation many times in the ensuing decade with essentially no success (35,36). The NRC identified vented-filtered containment systems as one of its five high priority items in its report to Congress on a program of research to improve reactor safety (32) but gave it very limited support prior to TMI 2.

There were two actions by the NRC in the mid-1970s, however, that did portend a possible shift from the previously long-held position of not looking beyond the design basis accidents. First, the Regulatory staff and Commissioners took steps to initiate emergency planning beyond the low population zone (37). Second, effects from a postulated core melt accident for the proposed floating nuclear plant were judged to be large enough to warrant design changes, even though this action was taken as part of the environmental review, not the safety evaluation (38).

TMI 2 may have speeded up what was an inexorable trend. However, prior to TMI 2, the pace was very slow and the end product uncertain. Since TMI 2, the pace has accelerated, although the outcome still remains to be determined.

In the fall of 1979 the NRC initiated studies related to the possibility of reducing risk from the Indian Point and Zion plants, which are located at the two most populated sites used for power reactors in the U.S. These studies involved a probabilistic look at accident initiators and an evaluation of design features that could mitigate the consequences of an accident leading to a highly degraded or molten core (39).

The ACRS recommended in December, 1979 that the NRC require the

licensee of each operating power reactor to perform design studies and examine the pros and cons of possible measures to mitigate core melt accidents (40). The ACRS reiterated this recommendation in September 1980; (22) it also recommended that measures for hydrogen control be implemented within about a year for PWRs employing the ice condenser containment, which has a smaller volume and much lower design pressure than the typical large, dry PWR containment.(41). The NRC adopted this latter recommendation in approving a full power license for Sequoyah.

I believe that design measures to cope with and mitigate core melt accidents should be given high priority, and that, assuming their positive features clearly outweigh any negative impacts, they should be implemented, as practical.

It appears likely, although by no means sure, that the NRC will require some improvement in the capability of Indian Point and Zion to cope with or mitigate the consequences of degraded core and core melt accidents. For other operating plants, for those near or under construction, and for plants to be designed, the pendulum could, in principle, swing either way, although I expect the trend to be in favor of mitigative measures.

In a speech given on July 9, 1980, NRC Commissioner Hendrie examined the existing NRC design basis accident approach (42). His remarks included the following comments.

"Some studies have already been undertaken of accidents beyond the design basis and of possible control measures, particularly in connection with the Commission's current review of high population density sites. It appears to me that current work on the course which extreme accidents might take indicates that for the great majority of such events there ought

to be enough time for offsite protective actions, including evacuation. But there may also be some practical plant design features that would give greater time for protective actions or reduce radioactivity releases and that would be appropriate for plants in high population areas. If this turned out to be the case, such plant design features should, as noted, be analyzed and treated on a best engineering calculation basis--in effect, a 'best effort' basis--rather than trying to include them in the design basis envelope."

"With the regulatory basis for reactor safety arranged in this fashion, we would have preserved the good features of the classical scheme and would have added to it the elements necessary to deal with most of its difficulties."

It remains to be seen whether these remarks by Commissioner Hendrie portend the extent of the application of mitigation measures for core melt accidents.

Regardless of whether or what new design features are implemented to mitigate degraded core and core melt accidents, analytical and experimental examination of the phenomena involved, and detailed studies of the course of various accident scenarios, are now receiving a high priority and can be expected to expand in breadth and depth. The kinds of effort underway since TMI include the following.

- the assessment by the NRC and by the licensees of the Zion and Indian Point pressurized water reactors of the course of various severe accident scenarios and the efficacy of various possible design features to mitigate the consequences (39).
- a detailed assessment of the capability of the Sequoyah ice-condenser type containment to withstand a hydrogen burning and

an evaluation of the efficacy of a hydrogen ignition system for a range of accident scenarios (43).

- a greatly expanded NRC safety research program on degraded core and core melt accidents (44).
- analysis of specific severe accident scenarios to ascertain whether the instrumentation currently being planned in Regulatory Guide 1.97 to help ascertain the course of an accident is subject to specific improvement (45).
- the proposed NRC rulemaking on degraded core and core melt accidents (46).
- the proposed NRC rulemaking on siting including the consideration of hydrological effects from serious accidents (47).
- the announcement that Class 9 accidents would no longer be excluded from environmental impact statements because of their low probability (48).

It is clear that the kinds of analysis underway on degraded core and core melt accidents are more detailed and sophisticated than that performed for the Reactor Safety Study, WASH-1400 (49). The interest now is on things like the coolability of a damaged or molten core; the pros and cons of large scale water addition; and the specific behavior characteristics and the pros and cons of various possible design measures to control hydrogen or containment overpressure. For other reasons, there is also likely to occur a much more sophisticated look than that in WASH-1400 of the economic effects of a large release of radioactive material and of the effects of such an accident on neighboring nuclear units and on water resources.

10. QUANTITATIVE SAFETY GOALS FOR THE NRC

The consideration of quantitative safety goals (or quantitative risk acceptance criteria) for LWRs preceded TMI 2 by some years (35). The ACRS recommendation, made several weeks after TMI 2, that the NRC pursue the development of such goals, resulted only in part from TMI 2 (56). Nevertheless, TMI 2 provided a situation which essentially required the NRC to look beyond its design basis accidents and to factor the risk of more severe events into its policies. Thus, the prevailing atmosphere became conducive to active consideration of quantitative safety goals by the NRC.

It is too soon to tell what, if any, quantitative safety goals the NRC will adopt, or how they may incorporate such goals into a broader safety policy for LWRs. However, serious discussion of various alternate approaches, an examination of the practicality and acceptability of specific numerical criteria, and an assessment of the impact of such an approach to risk management on both nuclear and non-nuclear technology, should contribute in many ways to the national debate on nuclear reactor safety and to the development of a modified safety philosophy for LWRs in the United States.

11. REGULATORY PHILOSOPHY

In the early 1970s, the point of view of the AEC regulatory staff was that the estimated frequency of an accident leading to core melt and containment failure, (which was identified as arising from a large LOCA, together with an independently occurring failure of the ECCS to function) was very low, of the order of 10^{-7} per reactor year (51). The estimated frequency of a very large release of radioactive material from a breached containment was taken by the regulatory staff to be of the order of 10^{-8} per reactor year (52).

When draft WASH-1400 in 1974 came up with an estimate of an overall core melt frequency of about one in 20,000 per reactor year (median value), the Regulatory Staff's first reaction was that the WASH-1400 core melt frequency was too high (49). Since issuance of the final version of WASH-1400 in 1975 with the same core melt frequency, a considerable number of things have occurred which tend to support a thesis that the WASH-1400 estimate of the frequency of core melt (or at least core damage severe enough to threaten containment and a major release of radioactive materials) was too low.

1) TMI 2 occurred with all of its insights into previously ill-considered or ill-regulated safety matters.

2) A re-evaluation by the NRC Staff of the failure rate data used in WASH-1400 in the light of new, more extensive data, suggests an increase by about a factor of three in the core melt frequency due to this effect alone (53).

3) The systematic evaluation program for ten old LWRs has shown deficiencies in these plants which could place them at a core melt frequency well above WASH-1400; some of the deficiencies are generic beyond the plants in this program (30).

4) Severe transients have occurred in operating plants via scenarios not envisaged in WASH-1400 (7,54). Several of these transients have had the potential to go to severe core damage, given another fault in the sequence.

5) Significant losses in safety system availability have occurred in operating plants. The Browns Ferry partial failure to scram has added further skepticism to industry claims of very high reliability of such safety systems (23).

6) It appears that while some systems interactions were considered in the WASH-1400 study, the scope of these considerations was inadequate. Similarly, the effects of control systems and other non-safety systems on accidents may not have received adequate attention.

7) The German risk study arrived at a core melt frequency larger than that of WASH-1400, after allowing for some modifications in the original PWR studied (55). The NRC studies of individual plants, such as the IREP results for Crystal River, have led to similar results (56).

8) The auxiliary feedwater studies performed after TMI 2 showed major weaknesses in reliability of this system for many existing plants (17).

9) Many design flaws have been uncovered in operating plants, some of them sufficient to lead to a severe core damage accident, given the correct initiating event.

10) Sabotage and flood were not included in the WASH-1400 estimates. Flood now appears to be a potentially significant contributor at some sites. Sabotage remains difficult to quantify, but there appears to be little basis for justifying it as small compared to a frequency of one in 10,000 per reactor year for a core damage accident.

11) The WASH-1400 evaluation that the seismic contribution to LWR risk is negligible has been shown to be in serious error (27). In addition, review of specific plant designs has turned up a wide range of design errors and other seismic deficiencies. Furthermore, estimates of the return frequency of the safe shutdown earthquake have become progressively larger with time so that they may now exceed those used in the WASH-1400 analysis.

For these and similar reasons, it appears to be difficult to demonstrate with a high degree of confidence that the frequency of severe core

damage or core melt for reactors in operation or under construction is less than about one in a thousand per year. It may be smaller, but it is also conceivable that it is somewhat larger. Also, there are many potential paths to severe core damage or core melt so that it will be difficult to make the frequency of such an accident very much smaller, with a high degree of confidence.

I am generally persuaded to be of this point of view, and as a consequence, would propose an overall safety philosophy which can be briefly summarized as follows:

1) For new reactors, choose the site so as not to impose an unnecessary risk to people or important resources.

2) Take all practical measures to reduce the likelihood of an accident which can seriously degrade the core and threaten containment of fission products.

3) Provide containment capability, as practical, for a wide spectrum of severe accidents as a separate line of defense, since it will be essentially impossible to know with the necessary very high degree of certainty that you have achieved a sufficiently low probability of preventing serious accidents to the core not to warrant mitigative measures.

4) Provide carefully and knowingly for emergencies, on-site in one's ability to ascertain the problem promptly and off-site by means of intelligent preparations.

I make these recommendations with full recognition that there are many risks in society, such as those from dams, from the storage of hazardous chemicals, and from the disposal of toxic wastes, that pose equal or greater risk to the individual and to society. The recommendations are also made

with the expectation that nuclear power plants currently introduce less statistical risk to the individual and society than most alternative forms of electricity, including the proposed new sources of the near or distant future. However, I think that there is a substantial body of public opinion which questions that the current level of safety is as good as is claimed and that there is a larger body of the public that wants nuclear power to be made more safe. I believe that it can be made more safe in a practical fashion, particularly if standardization is practiced for new plants and they are designed to have improved safety.

Appendix

ACRS RECOMMENDATIONS ON THE IMPLICATIONS OF THE THREE MILE ISLAND ACCIDENT

The ACRS has provided a series of recommendations covering a wide range of topics since the TMI accident, some of which are summarized below. Shortly after the accident, in a letter dated April 7, 1979 (57) the ACRS emphasized the importance of greatly increased knowledge of plant behavior during transients and accidents that involve small breaks in the primary system. The ACRS also emphasized the importance of additional information concerning plant status to the operator during an accident. In letters dated April 18, 1979 and May 16, 1979 (58,59), the ACRS emphasized, among other things, the importance of developing improved procedures and knowledge pertaining to the natural circulation cooling mode. In another letter dated May 16, 1979, the ACRS made a series of recommendations on topics including improved operator training and qualifications, improved operating procedures, and the need for early, industry-wide evaluation of operating experiences (60). The Committee also emphasized the importance of the reliability of AC and DC power supplies, and called for a re-evaluation of the single failure criterion.

In a letter dated May 16, 1979, the ACRS also recommended that the NRC give consideration to the establishment of quantitative safety goals (50).

In July, 1979, in its report NUREG-0603 on the safety research program (61) the ACRS made recommendations for major changes in the NRC safety research program. In a chapter entitled "Implications of the Accident at Three Mile Island, Unit 2," the ACRS called for new directions in research or major increases in previous priority for the following areas:

- anomalous transients and small LOCAs

- studies of the course of severe accidents
- molten core retention
- steam explosions
- siting
- plant operations
- transient simulation in research and licensing
- systems behavior and interaction
- application of probabilistic methodology
- disturbance analysis
- research to improve reactor safety.

In a letter dated August 14, 1979 (62), the ACRS made recommendations for studies on a large number of specific topics, for example, the potential role of air supplies in causing transients and accidents.

In a letter dated December 13, 1979 (40), the ACRS supported the bulk of the final report of the NRC lessons learned task force. The ACRS, however, recommended that, rather than the phased probabilistic reliability studies proposed by the staff in its IREP program, the NRC should develop a program in which each licensee assessed his plant using probabilistic techniques concurrent with the IREP program. The ACRS also recommended that each licensee be required to perform studies of possible hydrogen control and filtered-venting systems.

The ACRS also made several general recommendations in this letter including the need for improved shutdown heat removal systems and increased attention to the seismic qualification of auxiliary feedwater systems and the impact of an earthquake on non-safety systems.

In a long report entitled, "A Review of NRC Regulatory Processes

and Function," dated December 17, 1979 (10), the ACRS made a large number of major recommendations, including the following.

- the need for a systems approach to safety review and for a better audit of design
- the need for greatly increased industry ability to handle safety matters
- the need to consider accidents beyond the current design basis in deciding on the future approach to siting, design, and emergency measures
- modification of the single failure criterion
- the application of the probabilistic approach to design optimization for safety
- the need to consider the role of control systems and all other non-systems in safety, not just protection and engineered safety systems. (The ACRS reiterated this recommendation in its letter dated April 17, 1980 on the draft NRC Action Plan (63).)
- the need for a fundamental change in the approach and role of the architect engineer
- a change in orientation of the NRC safety research program from a primarily confirmatory role to one of improvement in safety and of exploratory efforts. (The ACRS reiterated this point in its report to Congress of February, 1980 on the NRC Safety Research Program, NUREG-0657 (64).)

A few other ACRS letters of particular interest during the same time period are as follows.

. comments on the report of the NRC task force on siting (65)

- letter to Commissioner Gilinsky on comparative risk of energy sources (66)
- letter to Commissioner Gilinsky on measures to mitigate core melt accident (67).

REFERENCES

[1] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USAEC, Letter to L. Manning Muntzing from W. R. Stratton, subject: Systems Analysis of Engineered Safety Systems (November 8, 1974).

[2] U.S. ATOMIC ENERGY COMMISSION, DIRECTORATE OF REGULATORY OPERATIONS, Notification of an Incident or Occurrence at Quad Cities Unit No. 1, #54 (June 12, 1972).

[3] U.S. NUCLEAR REGULATORY COMMISSION, NRC Action Plan Developed as a Result of the TMI-2 Accident, USNRC Rep. NUREG-0660 (1980).

[4] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Lee V. Gossick from Max W. Carbon, subject: Systems Interactions Study for Indian Point Nuclear Generating Unit No. 3 (October 12, 1979).

[5] FELKEL, L., et al., Analytical methods and performance evaluation of the STAR application in the Grafenrheinfeld nuclear power plant, Nuclear Power Plant Control and Instrumentation (Proc. Specialists Meeting Munich, 1978), IAEA, Vienna (1979).

[6] COMBUSTION ENGINEERING, INC., SYSTEMS CONTROL, INC., On-line Power Plant Alarm and Disturbance Analysis System, Electric Power Research Institute Rep. EPRI NP-1379 (1980).

[7] CASTO, W. R., Selected safety-related events reported in July and August 1978 - Common-cause incident involving nonnuclear instrumentation, Nucl. Safety 19 6 (1978) 765.

[8] CASTO, W. R., Selected safety-related events reported in March and April 1980 - Crystal River instrumentation and control failure, Nucl. Safety 21 4 (1980) 516.

[9] NUCLEAR SAFETY ANALYSIS CENTER, THE INSTITUTE OF NUCLEAR POWER OPERATIONS, Analysis and Evaluation of the Crystal River Unit 3 Incident, Nuclear Safety Analysis Center Rep. NSAC-3, The Institute of Nuclear Power Operations Rep. INPO-1 (1980).

[10] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, A Review of NRC Regulatory Processes and Functions, USNRC Rep. NUREG-0642 (1979).

[11] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. John F. Ahearne from Milton S. Plesset, subject: New Unresolved Safety Issues (August 12, 1980).

[12] U.S. NUCLEAR REGULATORY COMMISSION, Memorandum to H.R. Denton and C. Michelson from R. M. Bernero and F. H. Rowsome, subject: Single Failure Potentially Leading to Core Damage (March 14, 1980).

[13] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Joseph M. Hendrie from M. Bender, subject: Status of Generic Items Relating to Light-Water Reactors: Report No. 6 (November 15, 1977).

[14] ATOMIC SAFETY AND LICENSING APPEAL BOARD, USNRC, [Decision of July 30, 1980] In the Matter of Florida Power and Light Company, Docket No. 50-389 (St. Lucie Nuclear Power Plant, Unit No. 2), ALAB-603, Nucl. Regulatory Commission Issuances (in press).

[15] CASTO, W. R., Selected safety-related occurrences reported in March and April 1977 - Set point change produces unexpected results, Nucl. Safety 18 4 (1977) 551.

[16] U.S. NUCLEAR REGULATORY COMMISSION, Degredation of Engineered Safety Features, USNRC Office of Inspection and Enforcement IE Information Notice No. 70-04 (February 16, 1979).

[17] U.S. NUCLEAR REGULATORY COMMISSION, Report of the Bulletins and Orders Task Force, USNRC Rep. NUREG-0645 (1980).

[18] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. William A. Anders from William Kerr, subject: Reactor Safety Study, WASH-1400 (April 8, 1975).

[19] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Morris K. Udall from Dade W. Moeller, subject: [Reactor Safety Study, WASH-1400 (July 14, 1976).

[20] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Morris K. Udall from Dade W. Moeller, subject: [Reactor Safety Study, WASH-1400] (December 16, 1976).

[21] LEWIS, H. W., Chairman, et al., Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission, USNRC Rep. NUREG/CR-0400 (1978).

[22] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. John F. Ahearne from Milton S. Plesset, subject: Additional ACRS Comments on Hydrogen Control and Improvement of Containment Capability (September 8, 1980).

[23] U.S. NUCLEAR REGULATORY COMMISSION, Facility: Tennessee Valley Authority, Browns Ferry Unit 3, Docket No. 50-296, Athens, Alabama; Subject: Failure of Control Rods to Insert During a Scram, USNRC Preliminary Notification of Event or Unusual Occurrence PNO-II-80-119 (June 30, 1980).

[24] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS FELLOWS, USNRC, An Interim Report to the ACRS on a Review of Recent Malfunctions of BWR Scram Systems (August 8, 1980).

[25] U.S. NUCLEAR REGULATORY COMMISSION, Technical Report on D.C. Power Supplies in Nuclear Power Plants, USNRC Rep. NUREG-0305 (1977).

[26] FRANK, L., et al., Pipe Cracking Experience in Light-Water Reactors, USNRC Rep. NUREG-0679 (1980).

[27] HSIEH, T.-M., OKRENT, D., On design errors and system degradation in seismic safety, Structural Mechanics in Reactor Technology (Trans. 4th Int. Conf. San Francisco, 1977) Vol. K(b) paper K 9/4.

[28] U.S. NUCLEAR REGULATORY COMMISSION, Seismic Stress Analysis of Safety Related Piping, USNRC Office of Inspection and Enforcement IE Bulletin 79-07 (1979).

[29] U.S. NUCLEAR REGULATORY COMMISSION, Masonry Wall Designs, USNRC Office of Inspection and Enforcement IE Bulletins 79-02, 79-14, 79-28, 80-11 (1979, 1980).

[30] U.S. NUCLEAR REGULATORY COMMISSION, Letter from D. G. Eisenhut to Consumers Power Company (January 1, 1980).

[31] EBERSOLE, J. C., OKRENT, D., An integrated safe shutdown heat removal system for light water reactors, Nucl. Engr. and Design, 41 (1977) 421.

[32] U.S. NUCLEAR REGULATORY COMMISSION, Plan for Research to Improve the Safety of Light-Water Nuclear Power Plants, A Report to the Congress, USNRC Rep. NUREG-0438 (1978).

[33] U.S. NUCLEAR REGULATORY COMMISSION, Paper from Harold Denton to the Commissioners, subject: Special Report to Congress, Unresolved Safety Issues, USNRC Paper SECY-80-325 (July 9, 1980).

[34] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USAEC, Letter to Hon. Glenn T. Seaborg from David Okrent, subject: Report on Reactor Safety Research Program (October 12, 1966).

[35] OKRENT, D., On the History of the Evolution of Light-Water Reactor Safety in the United States, unpublished manuscript (1980).

[36] OKRENT, D., Nuclear Reactor Safety - On the History of the Regulatory Process, University of Wisconsin Press, Madison (in press).

[37] U.S. NUCLEAR REGULATORY COMMISSION, Upgraded Requirements for Emergency Response Plans, Federal Register 45 (August 19, 1980) 55402.

[38] U.S. NUCLEAR REGULATORY COMMISSION, Supplement No. 3 to the Safety Evaluation Report Related to Off-Shore Power Systems, Floating Nuclear Plant, USNRC Rep. NUREG-0054, Supp. No. 3 (1980).

[39] BERNERO, R. M., et al., Task Force Report on Interim Operation of Indian Point, USNRC Rep. NUREG-0715 (1980).

[40] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. John F. Ahearne from Max W. Carbon, subject: Report on TMI-2 Lessons Learned Task Force Final Report (December 13, 1979).

[41] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. John F. Ahearne from Milton S. Plesset, subject: Sequoyah Nuclear Power Plant, Units 1 and 2 (September 8, 1980).

[42] HENDRIE, J. M., "Nuclear safety and the regulation of nuclear technology", address before the First Texas Symposium on Energy, University of Texas at Dallas, Richardson, Texas (July 9, 1980) [reprinted in USNRC Office of Public Affairs News Releases, 6 28 (July 29, 1980) 10].

[43] U.S. NUCLEAR REGULATORY COMMISSION, Draft Supplement No. 3 [to the] Safety Evaluation Report Related to the Operation of Sequoyah Nuclear Power Plant, Units 1 and 2 (September, 1980) [to be published as Supp. No. 3 to USNRC Rep. NUREG-0011].

[44] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Comments on the NRC Safety Research Program Budget for Fiscal Year 1982, USNRC Rep. NUREG-0699 (1980).

[45] VON HERMANN, J., BROWN, R., TOME, A., Light Water Reactor Status Monitoring During Accident Conditions, USNRC Rep. NUREG/CR-1447 (EGG-EA-5153) (1980).

[46] U.S. NUCLEAR REGULATORY COMMISSION, Advance Notice of Rule-Making on Degraded Core Accidents, Federal Register (in press).

[47] U.S. NUCLEAR REGULATORY COMMISSION, Proposed rule making - 10 CFR Part 51 - Licensing and regulatory policy and procedures for environmental protection; alternative site reviews, Federal Register, 45 (April 9, 1980) 24168.

[48] U.S. NUCLEAR REGULATORY COMMISSION, Proposed rule making - 10 CFR Parts 50 and 51 - Statement of interim policy, nuclear power plant accident considerations under the National Environmental Policy Act of 1969, Federal Register, 45 (June 13, 1980) 40101.

[49] U.S. NUCLEAR REGULATORY COMMISSION, Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, USNRC Rep. WASH-1400 (NUREG-75/014) (1975).

[50] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Joseph M. Hendrie from Max W. Carbon, subject: Report on Quantitative Safety Goals (May 16, 1979).

[51] CASE, E.G., Analysis of a sudden major loss of coolant accompanied by serious failure of emergency core cooling[sic], Nucl. Safety 15 3 (1974) 285.

[52] U.S. ATOMIC ENERGY COMMISSION, Additional Guidance on Scope of Applicant's Environmental Reports with Respect to Accidents, USAEC Paper SECY-R 338 (November 15, 1971).

[53] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Morris K. Udall, from Milton S. Plesset, subject: [Actual Component Failure Experience] (February 20, 1980).

[54] CASTO, W. R., Selected safety-related events reported in January and February [sic] 1979-Loss of coolant inventory at Oyster Creek, Nucl. Safety 20 5 (1979) 623.

[55] GESELLSCHAFT FÜR REAKTORSICHERHEIT IM AUFTRAGE DES BUNDESMINISTERIUMS FÜR FORSCHUNG UND TECHNOLOGIE [CORPORATION FOR REACTOR SAFETY ON BEHALF OF THE FEDERAL MINISTRY FOR RESEARCH AND TECHNOLOGY], Deutsche Risikostudie Kernkraftwerke - eine Untersuchung zu dem Durch Stoerfaelle in Kernkraftwerken Verursachten Risiko [German Risk Study - A Study of Risk Induced by Accidents in Nuclear Power Plants]: U.S. Nucl. Regulatory Commission Translation 729, (May, 1980 [translation date]).

[56] SCIENCE APPLICATIONS, INC., Crystal River 3 Safety Study, (Draft), Science Applications, Inc. Draft Rep. SAI-002-80-BE (1980).

[57] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Joseph M. Hendrie from Max W. Carbon, subject: Interim Report on Recent Accident at the Three Mile Island Nuclear Station Unit 2 (April 7, 1979).

[58] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Memorandum to Commissioners from R. F. Fraley dated April 18, 1979 transmitting recommendations.

[59] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Joseph M. Hendrie from Max W. Carbon, subject: Interim Report No. 2 on Three Mile Island Nuclear Station Unit 2 (May 16, 1979).

[60] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Joseph M. Hendrie from Max W. Carbon, subject: Interim Report No. 3 on Three Mile Island Nuclear Station Unit 2 (May 16, 1979).

[61] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Comments on the NRC Safety Research Program Budget, USNRC Rep. NUREG-0603 (1979).

[62] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Joseph M. Hendrie from Max W. Carbon, subject: Studies to Improve Reactor Safety (August 14, 1979).

[63] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. John F. Ahearne from Milton S. Plesset, subject: NUREG-0660, "NRC Action Plans Developed as a Result of the TMI-2 Accident," Draft 3 (April 17, 1980).

[64] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program for Fiscal Year 1981, USNRC Rep. NUREG-0657 (1980).

[65] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. John F. Ahearne from Milton S. Plesset, subject: NUREG-0625, "Report of the Siting Policy Task Force" (February 14, 1980).

[66] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Victor Gilinsky from Milton S. Plesset, subject: [Technical Basis for Risk Comparison with Other Methods of Electricity Generation] (May 7, 1980).

[67] ADVISORY COMMITTEE ON REACTOR SAFEGUARDS, USNRC, Letter to Hon. Victor Gilinsky from Milton S. Plesset, subject: [Mitigation of Core Melt] (May 7, 1980).