REVIEW OF THE AMERICAN PHYSICAL SOCIETY LIGHT WATER REACTOR SAFETY STUDY

Robert J. Budnitz

Lawrence Berkeley Laboratory
University of California
Berkeley, CA 94720

INTRODUCTION

The issue of light-water reactor (LWR) safety has been the subject of a part-time, year-long study sponsored by the American Physical Society and supported by the National Science Foundation and the former Atomic Energy Commission. The goal of the study was the assessment of some of the technical aspects of the safety of large light water nuclear power reactors typical of present commercial practice in the United States. The 1974-1975 study produced a Report by the Study Group to the Society, which has been published in Reviews of Modern Physics, Volume 47, Supplement No. 1 (1975), and is available as a reprint for $6.00 from the American Institute of Physics (Reprint Department), 335 E. 45 St., New York, NY 10017.

The Report examines issues related to the safe operation of LWRs; the research and development program responsible for establishing and enhancing safety; and the consequences of accidents for public health and welfare. A number of recommendations are contained within the Report, mainly addressed to ways in which the safety of the present LWRs can be improved and better understood.

Robert J. Budnitz was one of the twelve Study Group participants, and his Invited Paper at the IEEE Nuclear Science Symposium covered many of the issues dealt with in the full Report. Because his remarks represent a brief review of the results of the full Study Group, it seems more appropriate to reproduce here the Report's "Summary of Conclusions and Major Recommendations." This reproduction follows below in full:

SUMMARY OF CONCLUSIONS AND MAJOR RECOMMENDATIONS

A central issue in the operation of light-water reactors is the prevention of a major release and widespread dispersal of radioactivity, which could have serious consequences to the public. The safety record of light-water reactors to date has been excellent, in that there has been no major release of radioactivity. These reactors have been designed with numerous safety features engineered to prevent foreseeable accidents. These safety features are backed up by other safety features intended to prevent major release of radioactivity in the event of an accident. Moreover, very conscientious efforts have been made in developing the procedures and practices involved in licensing, quality assurance, operation, and inspection of these reactors to insure sound construction and operation within specified safety limits.

In the course of this study, we have not uncovered reasons for substantial short-range concern regarding risk of accidents in light-water reactors. While at present a complete quantitative assessment of all important aspects of reactor safety and behavior under unusual circumstances cannot be made, we are confident that a much better quantitative evaluation and consequent improvements of the safety situation can be achieved over the next decade if certain aspects of the safety research program are substantially improved and the results of the research are implemented. Because of the serious potential consequences of a major release of radioactivity, and in view of existing safety-related technological opportunities, we believe that there should be a continuing major effort to improve light-water reactor safety as well as understand and mitigate the consequences of possible accidents. Our recommendations are directed towards these objectives.

A. Safety through careful design, construction, and operation

The safety philosophy of the nuclear industry has emphasized design which can provide tolerance against malfunctions. This approach has laid a good foundation for reactor safety, and it has resulted in reactors designed, constructed, and operated for safety, not only under normal operating conditions but also in a wide range of abnormal circumstances. A great deal of research, development, and quality control has gone into guaranteeing the integrity of the fuel elements and cladding, the integrity of the enclosing primary system, the general structural soundness of the entire reactor, and the ability to control the reactor under both normal and abnormal conditions.

Although we have not been able to analyze all of the many possible failure sequences for light-water reactors, one which we have studied in detail is the possible failure of the integrity of the primary reactor pressure vessel. We find that reactor vessels are constructed of materials chosen with care and are designed with substantial safety factors. The reactor vessel is subject to careful scrutiny and testing. Based on our study, we believe that catastrophic rupture of the primary pressure vessel is not likely to be an important contributor to accident initiation; however, this is dependent upon maintaining a strong quality assurance program.

Primary system piping is also subject to careful scrutiny and testing. The well-known cases of cracks in pipes and failures of valves in reactor operation, on the one hand, reflect deficiencies in fabrication or design; but, on the other hand, they demonstrate the success of the overall safety system and procedures which identified their existence early enough to prevent more serious consequences. Continued open discussion and analysis of such failures can lead to improvements in safety and can provide the data base for a more accurate estimate of the probability of more serious incidents. These defects underline the ongoing need for the nuclear industry and the regulatory bodies to continue improvement of inspection and test techniques. It is important that licensing and regulation be conducted in such a way as to continue to ensure openness in the quality assurance program and to provide better-quantified evaluation of the success of the program. We also note that each year human error on the part of reactor operators seems to initiate or aggravate at least a few incidents of potential safety significance. In fact, unless diligence is maintained, quality assurance and human error may well represent a limiting factor in maintaining safe operation.

It is difficult to quantify accurately the probability that any accident-initiating event might occur.

Many aspects need to be better understood through experience and research before such calculations are tractable. Although the probabilities of major accidents seem small their quantification deserves more attention within the reactor safety community than it has received up to now. We did not have the resources to carry out an independent evaluation of this aspect of the recent AEC Reactor Safety Study (Draft WASH-1400), but we recognize that the event-tree and fault-tree approach can have merit in highlighting *relative* strengths and weaknesses of reactor systems, particularly through comparison of different sequences of reactor behavior. However, based on our experience with problems of this nature involving very low probabilities, we do not now have confidence in the presently calculated absolute values of the probabilities of the various branches.

We have reservations about the present almost exclusive emphasis in the licensing process on the "design basis accident" concept in which certain highly stylized accidents are used as yardsticks against which the performance of various systems is evaluated. While we agree that analysis of such accidents is an important check upon the general safety of reactor designs, we are concerned that other types of possible accidents may consequently receive insufficient attention in design, construction, licensing, and operation.

B. Primary engineered safety features

In our study we centered much attention on the "engineered safety features." Because these features are not used in normal operation but are specifically intended to prevent an abnormal incident from becoming an accident, there is only limited operating experience with them. In addition, because of the complexity of the phenomena involved, these features are very difficult to simulate on a computer or to test in simulated accident conditions. Therefore, there is a lack of well-quantified understanding of the performance of some of these special systems under some severe accident conditions.

One of the most important of the engineered safety features is the fast-acting SCRAM system for shutting down the chain reaction in the event of an emergency. Certain transients which are anticipated to occur from time to time (pressure, temperature, reactivity) might play an important role in accident initiation. It is very important to shut down the chain reaction during a large transient. While the SCRAM designs, as now prescribed, seem to us to be highly reliable, not enough is known about the effects of transients in the extremely unlikely event that the reactor does not SCRAM. We believe that insufficient attention has been given to the analysis of transients, although it is encouraging that these areas are now being given intensive study. In addition, we are concerned about transient behavior which might occur simultaneously with a massive electrical failure. While there are redundant off-site power sources, the emergency on-site (diesel) power sources are a recognized weak point.

The emergency core cooling system (ECCS) is the engineered safety feature that has received the most publicity, attention, and research. The ECCS is intended to provide emergency cooling to prevent the reactor fuel from melting or losing structural integrity in the event there is a loss of primary system fluid.

We have no reason to doubt that the ECCS will function as designed under most circumstances requiring its use. However, no comprehensive, thoroughly *quantitative* basis now exists for evaluating ECCS performance because of inadequacies in the present data base and calculational codes. In addition, it is not clear that the present approximate calculations, even though based on generally conservative detailed assumptions, will in all cases yield conservative assessments of ECCS performance.

We have examined the AEC reactor safety research program intended to resolve these uncertainties. Expanded experimental tests and advanced calculational code development are now under way, with the goal of accomplishing a sufficient quantitative comparison between calculation and experiment so that the technical community can reach consensus on ECCS effectiveness. That consensus can only be reached through several years of effort, using improved research techniques, and with more open publication and review of the results. We doubt that a complete quantitative evaluation of ECCS effectiveness can be achieved through the present program. We recommend below several possible approaches for improvement.

C. Accident containment and consequences

The last line of defense in preventing or mitigating the release of radioactivity is a further set of engineered safety features designed as a backstop in case of significant failure of the safety features discussed above. The greater part of this last safety umbrella is the containment machinery and building which enclose the entire reactor primary system. These containments, which have worked well in controlling routine and minor radioactive emissions, have not yet been subjected to test by a large-scale controlled or accidental release. More research toward increasing the effectiveness of containment devices would be prudent, along with more vigorous pursuit of the possibilities for major improvements in containment design.

Although a major release of radioactivity is unlikely, it is important to calculate the types and extent of consequences of releases under various circumstances. We have found that these calculations are very difficult. There are significant uncertainties in nearly every category of potential consequences: immediate deaths, latent cancers, and property damage/denial. We have made no independent studies of acute effects, the estimates of which are particularly dependent upon details of local siting, weather, and population, and upon important uncertainties in acute biological effects of radiation. However, for the same releases and the same basic references for the biological effects as taken in Draft WASH-1400, we estimate substantially larger long-term consequences, particularly concerning land damage/denial and possible latent cancers from exposures to individuals who live in areas which are contaminated below the evacuation thresholds used in Draft WASH-1400.[2] The social significance of the long-term consequences depends in part upon the probability of the assumed release, regarding which we have made no independent assessment. However, the uncertainties in estimates of consequences need to be resolved because they have important implications in reactor design, siting policy, and protection against potential sabotage. In analyzing the societal risk-benefit balance of commercial nuclear reactors, one must be able to estimate with reasonable confidence both the probability and consequences of system failure; research must continue on both.

Considering the great social importance of reactor safety and the large present and future capital investment in light-water reactors, the current funding of safety research is relatively small. We believe that the many technological opportunities for the enhancement of reactor safety warrant the investment of additional funds in safety research.

D. Major recommendations

Many recommendations are made in the body of this Report. A few of the major ones are summarized here, but in each case the reader is referred to the main text for detailed discussions of the background and rationale. Our major recommendations, which have not been ranked according to their importance, include the following:

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

(2) Measures should be taken to quantify the effectiveness of the present quality assurance program, using both the analysis of experience already reported and new measurements on the quality assurance system.

(3) The techniques used in Draft WASH-1400 for the calculation of accident sequences and their probabilities should be:

- employed to estimate quantitatively whether assumed subsystem failure data are compatible with the observed individual small accidents;
- used to provide parametric studies of the effects of phenomena which are ill-understood in the identified sequences;
- refined so that they can be used for continuing risk assessment on a routine basis with a growing data base of failure data.

(4) The Draft WASH-1400 analysis of accident consequences should be redone taking into account the modifications discussed in our report, in order to obtain corrected consequence estimates. The results will help to determine the magnitude of the benefits which might be obtained from the introductions of design changes and means of mitigation of accident consequences.

(5) The problem of sabotage and its effect on increasing the risk of radioactivity release should be studied carefully. We have no way of estimating the present likelihood of sabotage; however, we believe that reactor security can be improved and have specific recommendations for studies that go beyond those already underway.

(6) The ECCS safety margin should be quantified, and if necessary, improved through one or more of the following approaches:

- the substitution of more easily analyzable or more effective ECCS concepts;
- a much stronger theoretical and calculational development effort combined with a much improved experimental program, the results of which must be published openly for evaluation by the technical community;
- a series of large-scale experiments along with some standardization of reactors. Detailed planning and analysis for this approach should begin immediately in case it should be decided in the future that it is needed. There should be increased emphasis on realistic calculations and experiments as opposed to those which merely attempt to set upper limits on the behavior of a reactor in an accident. In view of the number of reactors now operating and being planned we believe it is important that the reactor safety research program quickly take major steps to bring about a convincing resolution of the uncertainties in ECCS performance.

(7) In the area of safety research, more emphasis should be placed on seeking improvements in containment methods and technology. In particular, controlled venting of the containment building in case of overpressure should be studied. A careful assessment should also be made of the benefits and costs of alternative siting policies, such as remote, underground, and nuclear-park siting.

(8) There should be more effort to resolve major uncertainties in estimating consequences, including improvement of the biological-effects data base. Techniques for mitigation of consequences should be developed, especially in connection with the problems of decontamination after a large accident.

(9) While we strongly endorse the substantial improvements that have been made in the safety research programs and in the openness to scrutiny by the technical public in the last two years, additional measures should be taken to continue to improve the research program and techniques and to assure that the results of both experimental and computer code development work related to safety are openly published.

FOOTNOTES

[1]Funding for this study was through the United States Energy and Resources Development Administration.

[2]We understand that substantial revisions are being considered before publication of the final WASH-1400 report (private communication, Nuclear Regulatory Commission, 17 March 1975).