WASH–1400
(NUREG 75/014)

REACTOR SAFETY STUDY

AN ASSESSMENT
OF ACCIDENT RISKS
in
U.S. COMMERCIAL NUCLEAR POWER PLANTS

U.S. NUCLEAR REGULATORY COMMISSION
OCTOBER 1975

Foreword

This is the final report of the Reactor Safety Study "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," prepared under the direction of Professor Norman C. Rasmussen of the Massachusetts Institute of Technology. The work, originally sponsored by the U.S. Atomic Energy Commission, was completed under the sponsorship of the U.S. Nuclear Regulatory Commission which came into being on January 19, 1975.

A draft report was published in August of 1974 and was circulated to obtain comments from a wide variety of people and organizations. Comments were requested from other agencies of the federal government, environmental groups, groups critical of nuclear power, lawyers representing environmental groups and industry, and industrial organizations representing reactor manufacturers, architect engineering firms and electric utilities. In addition to this distribution, many requests for the report were received from other individuals and organizations. A total of about 90 letters of comment were received which were very helpful in the preparation of this final report. A new Appendix XI has been added to the report to indicate the study's responses to the comments received and the resulting changes made in the final report.

The Reactor Safety Study was performed, as described in Chapter 1, by an ad hoc group of people initially assembled by the Atomic Energy Commission to do an independent assessment of potential accident risks in U.S. commercial nuclear power plants. When the U.S. Nuclear Regulatory Commission was created in January of 1975 the work continued under its auspices with renewed re-emphasis on the independent nature of the study group.

The study group wishes to thank all those who contributed to the support of the effort and the technical work as well as those who commented on the draft report to help improve the quality of the final version.

Main Report

Table of Contents

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

List of Tables

List of Tables (Continued)

List of Figures

List of Figures (Continued)

List of Figures (Continued)

Chapter 1

Objectives and Organization of the Reactor Safety Study

1.1 INTRODUCTION

Although nuclear power plants have advantages over fossil plants in most areas of environmental effects and in the cost of electricity, they have some potential for accidents with larger public consequences than fossil-fueled plants. While the safety of nuclear plants has been much discussed in nuclear circles for more than twenty years, it has only recently attracted wider interest. Much confusion exists in this area principally because the published results of early studies[1] have been widely misunderstood and because no recent assessment of reactor risks has been made. The principal purpose of this study is to assess the risks to the public from potential accidents in nuclear power plants of the type being built in the United States today. It is intended that the present study will produce a more realistic assessment of these risks than has been provided in earlier work; it may also help to dispel some of the existing confusion.

It is important to understand that the earlier studies of nuclear power plant accidents were performed with objectives other than realistic risk assessment in mind. The AEC's major early study, published in 1957, was performed by Brookhaven National Laboratory (BNL) and was entitled "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants." Its objective was to provide an estimate of the upper limit to the consequences that might be involved in such accidents in order to help the Congress ensure that legislation being considered to provide government indemnification of the public would be adequate. It is of interest that, at the time of the BNL study, only a few very small military power plants existed and no commercial nuclear power plants were in operation, although some were being designed and constructed. Furthermore, techniques for predicting the likelihood of failure of engineered systems had not been well developed. Clearly, even if the reliability techniques needed for risk assessment had been available, the engineering information needed to draw meaningful conclusions about the probability of accidents in future plants did not exist.

For these reasons, the 1957 effort devoted little attention to the probability of occurrence of accidents. In the past 10 years the development of reliability techniques has progressed considerably. Further, as a result of the increased use of commercial nuclear power plants in the last decade, a well-developed approach to the safety design of water-cooled reactors and specific engineering designs needed to implement a quantitative approach to risk assessment now exists.

1.2 OBJECTIVES OF THE REACTOR SAFETY STUDY

At the start of the Reactor Safety Study in the summer of 1972, there was considerable uncertainty about the applicability of reliability techniques to quantitative risk assessment and about the ability of these techniques to achieve credible estimates of the occurrence of events of low probability. Experience had indicated that application of these techniques generally led to estimates of failure of engineered systems that were so small as to contradict common experience. Much of the uncertainty that existed is exhibited in the statement of objectives given to the Reactor Safety Study by the Atomic Energy Commission on August 4, 1972:

"The principal objective of the study is to try to reach some meaningful conclusions about the risks of nuclear accidents using current technology. It is recognized, however, that the present state of knowledge probably will not permit a complete analysis of low-probability accidents in nuclear plants with the precision that would be desirable. Where this is the case, the study will consider the uncertainty in present knowledge and the consequent range in the predictions, as well as delineating outstanding problems. In this way, any

[1] WASH 1250, Chapter 6, summarized some of this early work.

uncertainties in the results of this study can be placed in perspective. Thus, although the results of this study of necessity will be imprecise in some aspects, the study nevertheless will provide an important first step in the development of quantitative risk analysis methods."

As confidence within the study group grew in the ability to achieve a meaningful risk assessment, the Reactor Safety Study added the following more specific objectives under its original, broadly stated charter:

a. Perform a quantitative assessment of the risk to the public from reactor accidents. This requires analyses directed toward determining both the probabilities and the consequences of such accidents.

b. Perform a more realistic assessment as opposed to the "conservatively-oriented" safety approach taken in previous studies of this type and the licensing process for nuclear power plants.

c. Develop the methodological approaches needed to perform these assessments and gain an understanding of their limitations.

d. Identify areas in which future safety research might be fruitfully directed.

e. Provide an independent check of the effectiveness of the reactor safety practices of industry and the government.

1.3 ORGANIZATION OF THE REACTOR SAFETY STUDY

The study was organized to be independent of the AEC's operating and regulatory organizations. Professor Norman C. Rasmussen of MIT, as Director of the Reactor Safety Study, reported to the Commission. While funds and such other assistance as were needed were provided by the AEC, the study operated under the general charter provided by the Commission, but received no other direction from it.[1]

To assist Dr. Rasmussen in the technical management of the study, the AEC assigned Saul Levine as Project Staff Director. In addition, one part-time and seven full-time participants were AEC employees. One participant was from the operational side of the AEC to assist in matters involving design and the others, on loan from the AEC's regulatory staff, were technical safety specialists with detailed knowledge of reactor plants. Additional participants were furnished by contractors and national laboratories to fulfill the specialized technical needs of the study. Some of the organizations and their field of expertise were:

a. Boeing Company-Fault tree analysis.

b. Aerojet Nuclear analysis.

c. Science Applications, trees and event trees.

d. Lawrence Livermore Laboratory-Fault tree analysis.

e. Sandia Laboratories-Data analysis, fault tree analysis and consequence modeling.

f. Oak Ridge National Laboratory-Systems engineering analysis.

g. Teknekron-Technical editing.

h. Hanford Engineering Development Laboratory-Consequence modeling.

The work by the above organizations was performed almost entirely at AEC Headquarters under the direction of Dr. Rasmussen and Mr. Levine.

In addition, work was contracted to other organizations not located at Headquarters. However, it was directed in considerable detail by the Reactor Safety Study. Included were:

a. Battelle Columbus Laboratory-Radioactivity release and transport; analysis of molten fuel interactions.

b. Battelle Pacific Northwest transport.

c. Oak Ridge National Laboratory-Radioactivity release and transport; safety design rationale.

d. Aerojet Nuclear Company-Radioactivity release and transport.

[1] This same independence was preserved by the U.S. Nuclear Regulatory Commission when it assumed sponsorship of the study on January 19, 1975.

e. Franklin Institute Research Laboratories-Design adequacy.

f. University of California, Los Angeles-Other risks.

g. Lawrence Livermore Laboratory-Meteorological modeling.

h. Brookhaven National Laboratory-Health effects.

i. Oak Ridge Associated Universities-Health effects.

Other contracts involved small consulting efforts at Massachusetts Institute of Technology and National Oceanic and Atmospheric Administration on plume rise modeling, Stanford Research Institute on probability theory, and Institute of System Sciences on fault tree analysis.

In addition to those listed above, a group of consultants provided assistance in the health effects area. The constitution of this group is described in Appendix VI.

1.4 ORGANIZATION OF THE REPORT

This report is organized as follows:

Chapter 1-Introduction.

Chapter 2-Basic Concepts of Risk. Discusses various concepts involved in risk assessment, covering the probabilities and consequences of accidents, societal and individual risks, attitudes toward risk and quantitative measures of risk.

Chapter 3-The Nature of Nuclear Power Plant Accidents. Identifies radioactivity in the core and elsewhere in the nuclear power plant as a source of potential risk and describes ways in which this radioactivity could be released to become a potential risk to the public.

Chapter 4-Risk Assessment Methodology. Explains the methods used in defining accident sequences and in determining their probability of occurrence and the associated releases of radioactivity. Describes development and evaluation of event trees and accident sequences, the use of fault trees to predict probabilities of event occurrence and of system failures, and the development of a model to calculate the consequences of accidents.

Chapter 5-Reactor Accident Risks. Presents the estimated quantitative risks associated with reactor accidents. The results of the major effort involved in the study are given in this chapter.

Chapter 6-Comparison of Risks. Presents a compilation of non-nuclear risks and a comparison with the nuclear reactor risk developed in this study. Non-nuclear risks include other technological risks and those due to natural phenomena.

Chapter 7-Conclusions and Recommendations. Summarizes the evaluation of risks, remarks on the validity and limitations of this study, discusses areas where further investigation would be appropriate, and presents the principal insights gained in the study.

Addendum I-An Overview of Event Tree and Fault Tree Methodology and the Handling of Common Mode Failures. Presents an overview and discussion of the impact of the event trees and fault trees, and failure data in the definition and quantification of accident sequences. The handling of potential common mode failures is emphasized.

1.5 TECHNICAL APPENDICES

The Reactor Safety Study report has ten appendices which document in considerable detail the technical work done in connection with the study. This amount of detail is presented for two reasons. The first is to document the work done, especially because many areas of the study, such as event trees, quantification of fault trees, contributions due to common mode failures, and the consequence model, represent some extension of the techniques associated with reliability analysis and risk assessment. The second is to provide interested readers with sufficient detail to enable them to make a critical review of the study. An eleventh appendix documents the study's reaction

to the comments received on the draft report. The appendices involved are:

Appendix I-Accident Definition and Use of Event Trees.

This appendix contains a description of event tree methodology as used in the study and its role as the principal tool in defining complex accident sequences. It also contains a discussion of the potential accidents explored in the study and presents the event trees used. See Chapter 3.

Appendix II-Fault Trees.

Methodologies used in constructing and quantitatively assessing fault trees are presented along with the results of the quantification of the fault trees used in this study. Individual reports describing the fault tree evaluation of the plant systems analyzed are also presented. See Chapter 4.

Appendix III-Failure Data.

This appendix contains a compendium of data sources and data used in the quantitative evaluation of fault trees and event trees. See Chapter 4.

Appendix IV-Common Mode Failures.

The techniques used in the study to analyze the possible contributions of common mode failures to overall risk assessment are summarized. See Chapter 4.

Appendix V-Quantitative Results of Accident Sequences.

The probabilities of occurrence combined with the radioactive releases for the accidents defined in Appendix I are presented. Also included is the ordering of accident sequences to identify those sequences that are the major contributors to the various sizes of releases. See Chapter 5.

Appendix VI-Calculations of Reactor Accident Consequences.

The model used for predicting the dispersion of radioactivity in the environment is presented, together with the models for predicting the results of this dispersion in terms of fatalities, injuries, long term health effects, and property damage. See Chapter 5.

Appendix VII-Release of Radioactivity in Reactor Accidents.

The factors affecting the magnitude of the release of radioactivity from fuel under various conditions determined by the accident sequences are presented, as are the transport and removal mechanisms that affect the releases of radioactivity from the facility. See Chapter 5.

Appendix VIII-Physical Processes in Reactor Meltdown Accidents.

The various engineered safety feature interactions as defined by the accident sequences are described. Included are predictions of core and containment behavior, along with times of fuel melting, times and modes of containment failure, and the interactions of molten fuel and cladding with water and concrete. See Chapters 3 and 4.

Appendix IX-Safety Design Rationale for Nuclear Power Plants.

A discussion of the safety design rationale currently used for pressurized and boiling water reactors is presented. It includes a discussion of the barriers to the release of radioactivity and their design bases, a discussion of potential accident initiators in nuclear power plants, and the features provided to mitigate the effects of these accident initiators.

Appendix X-Safety Design Adequacy of Nuclear Power Plants.

A study of the extent to which safety design requirements in regard to seismic and accident environments have been fulfilled in the actual engineering design of the plants. See Chapter 5.

Appendix XI-Analysis of Comments on the Draft WASH-1400 Report.

This appendix contains a discussion of the comments received as a result of the draft report.

1.6 REACTOR SAFETY STUDY FLOW CHART

Figure 1-1 is a simplified flow chart of the work done in the Reactor Safety Study.[1] The first step in the work was to define those failures in nuclear power plants that could lead to potential risks to the public. This involved determining the locations and sizes of all sources of radioactivity in the plant and then describing the various combinations of equipment and human failures that could potentially cause the release of some portion of this radioactivity. The combinations of failures involved in the potential release of radioactivity are called accident sequences and were principally determined by event trees (Appendix I) and by the analyses associated with molten core behavior (Appendix VIII).

The second step in this study was the estimation of the probability of occurrence of the accident sequences and the amounts and types of radioactivity released by these sequences. Fault trees and failure data (Appendices II and III), together with common mode failure investigations (Appendix IV), are used to estimate the failure probabilities. Analysis of experimental data and fuel conditions (Appendices VII and VIII) provided estimated releases of radioactivity. Appendix V presents the compilation of probabilities and radioactive releases for accident sequences.

The next step involved the use of a probabilistic model to calculate the dispersion of radioactivity in the environment. This model (Appendix VI) also includes the factors necessary to compute health effects and property damage due to the dispersion of radioactivity.

The final step covered the overall assessment of the nuclear accident risks (Chapter 5) and a comparison of these with non-nuclear risks due to natural phenomena and other technologies (Chapter 6).

1.7 FACTORS THAT CONTRIBUTED SIGNIFICANTLY IN PERFORMING THE STUDY

As indicated earlier, there was initially some doubt that a meaningful risk assessment could be made; however, as the work proceeded, confidence grew in the ability to make a meaningful risk assessment. The principal factors that contributed to this change are discussed below:

a. The study was started with the idea of using standard fault tree methodology as the principal tool for developing both the accident sequences and their probabilities. It soon became apparent that this approach was not adequate for the entire task. While well suited to predicting probabilities of failure for engineered systems, it is not well adapted to defining accident sequences that involve the complex interrelationships among engineered safety systems in nuclear power plants. Thus, in order for the study to proceed, it was necessary to use a method that could fulfill this need. The use of event trees, discussed in detail in Appendix I and in Addendum I to the Main Report resolved this problem.

b. The question of the adequacy of data pertinent to equipment failures and human errors also represented a potential stumbling block for the study. Many people view the lack of precision in failure rate data as one of the pitfalls of quantitative reliability analysis. They also extend this view to risk assessment without recognizing an important difference between the two. In reliability analysis, one is generally interested in predicting a particular level of reliability with a relatively high degree of accuracy. One is also interested in identifying differences in the reliability of alternate designs. This generally requires analyses that have small errors (for example, less than a factor of three). In risk assessment one can accept whatever level of accuracy is obtainable from available data and then examine the results to see if they are meaningful. In fact, for small probabilities such as those projected for nuclear accidents, rather large errors (a factor of 10 or more) can often be tolerated without materially reducing the usefulness or validity of the result. Since risk assessment can tolerate large error bands in its quantitative results, the dependence of this study on precise values of failure rate data was greatly reduced. Also, the availability of many sources of data for the types of components used in nuclear plants and the confirmation of some of these data with available nuclear

[1] Detailed flow charts are presented in Chapter 4.

component data did much to resolve this issue. The data base and its use in the study are discussed in Appendix III.

c. The most uncertain area in the study related to whether potential common mode failures or dependent failures, could be properly identified.[1] The approach taken from the beginning of the study was to consider the dependencies involved in the assignment of failure probabilities. However, given the number of potential accident sequences possible in a reactor and the number of components involved in all of the systems in these sequences, the number of interactions that might have to be examined for potential common mode failures seems at initial glance to be beyond any realistically obtainable capability. Nonetheless, it is believed that the work performed in this study has, by a combination of methods involving event trees, fault trees, mathematical techniques and engineering studies, eliminated the vast majority of potential interactions as not significant and has examined the remainder in sufficient detail to define common mode contributions where they are important. A complete discussion of common mode failures is contained in Addendum I to the Main Report and in Appendix IV.

d. A review of previously performed estimates of the likelihood of failure of engineered systems reveals that they generally predicted probabilities that were quite small compared to real experience. If techniques used in such previous estimates had been followed in this study, predictions of the likelihood of reactor accidents and system failures would have been so small as to be equally unbelievable. A determined, large scale effort was made in this study to ensure that the techniques used would produce meaningful estimates. To accomplish this purpose, the significant dependencies between failures were carefully considered by a combination of engineering and mathematical techniques. Some measure of the success achieved by this effort, as indicated in Appendix II, is that estimated system failure probabilities closely matched experience data in those cases where measured values existed.

1.8 INSIGHTS GAINED DURING THE STUDY

The major effort in reactor safety in the past few decades has been devoted to the prevention of overheating and melting of the nuclear fuel in reactors. This approach was necessary because it was recognized that an accident with large public consequences could occur only as a result of melting the fuel in a reactor core. However, much less attention was devoted to analysis of the consequences of core melting. The principal effort in this study has been devoted to accidents in which core melting could potentially occur and to the consequences of such accidents. The insights gained from this effort are as follows:

a. The work in this study has shown that melting of the reactor core does not necessarily result in an accident having large public consequences. Indeed, in the unlikely event that a core were to melt, there is a spectrum of possible accidents that can occur.

b. For the most likely course of events following the melting of a core, the number of fatalities expected is much smaller than those that commonly occur in accidents such as fires, explosions and crashes of a commercial jet airplane. In addition, the likelihood of core melt is calculated to be much smaller than any of the above.

c. Previous analyses of the consequences of reactor accidents have generally emphasized those that could occur under conditions of poor atmospheric dispersion and in locations involving relatively high population densities. In actuality, there are wide varieties of weather conditions and population densities where reactors are located. When appropriate frequencies of occurrence are assigned to weather conditions and population densities, these can cause potential accident consequences to increase by 100 to 1000 times; however, the probability of such accidents could decrease by generally similar factors.

---

[1] In a simplified way, common mode failures can be thought of as multiple failures caused by a single event or failure, e.g., the same environmental condition.

1.9 LIMITATIONS IN THE STUDY

As indicated earlier, this study covers only light water cooled nuclear power plants of the type now coming into operation. It is understood that future studies by the AEC will cover risk assessment of advanced reactors such as high temperature gas cooled reactors and liquid metal fast breeder reactors.

Two plants were used as the basis for the study, a PWR and a BWR. The plants chosen were the PWR Surry Power Station, Unit 1, 788 Megawatts electrical capacity, and the BWR Peach Bottom Atomic Power Station, Unit II, 1065 Megawatts electrical capacity. The basis for their selection was that they were the largest plants of each type that were about to start operation. A question which must be considered is the applicability of the results obtained for these plants to nuclear power plants generally. Certainly the differences in design between various plants make this an appropriate question. It is the study's understanding that additional work will be done in the future to determine the applicability of the study results to water power reactors as a class. However, the following factors indicate that the study results, when extrapolated to 100 nuclear power plants, as has been done in this study, will tend to overestimate, rather than underestimate the risk. Of the large commercial nuclear power plants currently operating, the two plants covered in the study represent the 24th and 34th to come into operation.[1] Their designs were started in 1966. The 100th plant expected to commence operation had its design started in 1971. In the years between 1966 and 1971, significant improvements were made in the AEC's safety design requirements and their implementation and in the applicable codes and standards used in the design of nuclear power plants. It has already been observed in other technologies such as automobiles and airplanes that safety has generally improved with the passage of time.[2] Much of this improvement is due to continued attention to improved safety. Because of the existing record of improved safety requirements in nuclear power plants, it is not unreasonable to assume that the safety of nuclear power plants will continue to improve. This assumed improvement depends strongly on the continuing existence of competent and well supported regulatory and reactor safety research programs and reasonably conservative extrapolation of current practice. If the safety of nuclear power plants continues to improve with time then it would not be appropriate to extrapolate the results of this study beyond 100 reactors and about 5 years since the extrapolation would yield unrealistically high values.

The question of the effect of sabotage on nuclear power plants should be mentioned. The study was requested by many sources to examine this question; however, it could not be completely covered because no convincing way could be found to estimate the probability of acts of sabotage directed at any target. However, the study believes that nuclear power plants would be difficult to sabotage in the sense of creating an accident with large public consequences, clearly continuing precautions must be taken to minimize this potential. Some measures are already provided and improvements are underway. It is understood that the NRC is contemplating further improvements in the security of nuclear power plants.

1.10 FINAL REMARKS

This report provides considerable background for gaining an understanding of the concepts involved in risk assessment and of the elements involved in nuclear power plant safety. The results of the study of nuclear reactor accident risks are presented and compared with risks due to natural phenomena and other technologies in our society in order to provide perspective on low probability risks. A large amount of information has been developed in conducting the study and most of it is presented in this report and its appendices. It is expected that this information will be of use in making the controversy about reactor safety more objective. Obviously, the question of the acceptability of nuclear accident risks requires a much broader social judgment that transcends the scope of the Reactor Safety Study.

---

[1] These numbers exclude plants with capacities less than 400 megawatts electrical.

[2] See Chapter 2 for data on the safety record of airplanes and automobiles.

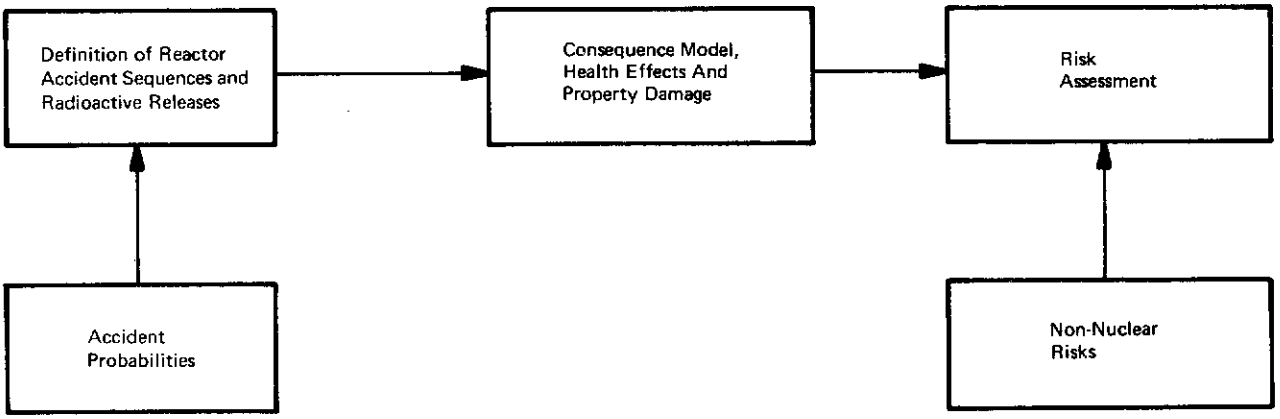


FIGURE 1-1 Reactor Safety Study Flow Chart

Chapter 2

Basic Concepts of Risk

Information about risks to the public health and safety has been collected for many years and provides a general indication of the risks normally encountered in our society. However, much less information is available on low probability risks with potentially high consequences such as those that might arise from nuclear power plant accidents or other sources. In the past, very little effort has been devoted to estimating the probability of such risks as they affect our society. Further, in most prior studies of potential large nuclear reactor accidents, the analysis of consequences has been done on an upper limit basis. This type of approach is not suitable for placing such risks in proper perspective with respect to the more common risks encountered by society. The purpose of this chapter is to define enough of the elements contributing to risk to make it easier to understand the risk assessments presented in later chapters.

2.1 MEASUREMENT OF RISK

Risk is a commonly used word that can convey a variety of meanings to different people. A dictionary definition is "the possibility of loss or injury to people and property". In this study estimates are made of potential fatalities and injuries to people and of property damage resulting from both nuclear power plant and non-nuclear accidents.

Particular emphasis will be placed on the risk to the health and safety of the general public.

To provide a basis for the quantitative comparison of societal risks from accidents, the following technical definition of risk is used:

$$\text{Risk} \left\{\frac{\text{consequence}}{\text{unit time}}\right\}$$

$$= \text{Frequency} \left\{\frac{\text{events}}{\text{unit time}}\right\}$$

$$\times \text{Magnitude} \left\{\frac{\text{consequences}}{\text{event}}\right\}$$

As a quantitative example of the use of such an equation, in 1971 about 15,000,000 auto accidents occurred in the U.S., and one in 300 accidents resulted in a fatality. Thus, the societal risk of death from auto accidents can be approximately calculated as:

$$15 \times 10^6 \frac{\text{accidents}}{\text{year}} \times \frac{1 \text{ death}}{300 \text{ accidents}}$$

$$= 50{,}000 \frac{\text{deaths}}{\text{year}}$$

Further, if U.S. society consists of 200,000,000 people, the average individual risk can be expressed as:

$$\frac{50{,}000 \text{ deaths/year}}{200{,}000{,}000 \text{ persons}} = \frac{2.5 \times 10^{-4} \text{ deaths}}{\text{person-year}}$$

The final term expresses the individual risk as probability of death per person per year. This mode of expression is frequently used in the mathematical analysis of risks. (For the benefit of those readers who are not familiar with such mathematical expressions of probability, a few words of explanation are provided in the "Notes on Probability".)

In the aforementioned example pertaining to fatalities in auto accidents, note that the risk is expressed both in terms of risk to society and risk to an individual. Additional risks due to auto accidents result from injuries and property damage. In the U.S. about 30 times as many people are seriously injured as are killed in auto accidents. Thus, on the average one person is injured in every 10 accidents. This yields, for societal risk,

$$15 \times 10^6 \frac{\text{accidents}}{\text{year}} \times \frac{1 \text{ injury}}{10 \text{ accidents}}$$

$$= 1{,}500{,}000 \frac{\text{injuries}}{\text{year}}$$

and, for individual risk,

NOTES ON PROBABILITY

In a one-winner lottery with a million ticket holders, and assuming a random selection of the winner, each ticket holder has the right to expect an equal chance of winning, but he will also know that his chance is only one in a million. In the mathematics of probability, this chance is expressed by the fraction: 1/1,000,000, which can also be written as 1×10^{-6} or 0.000001.

Similarly, an accident fatality rate counted at 25 persons per hundred thousand per year can be expressed as $25/100{,}000 = 25 \times 10^{-5} = 2.5 \times 10^{-4}$ or 0.00025. If it is assumed that all persons in the population have equal exposure to the risk of death from the type of accident under consideration, then these numbers mean that the chance of death per year is 25 per 100,000 persons, or 2.5 chances per year per 10,000 exposed persons, or 0.25 chances per 1,000 persons, or 0.00025 per one person.[1] The fractional numbers obviously have no physical meaning (since only a whole person dies), but they are useful in mathematical analyses of risk.

[1] In using the word "chance" in this context, it must be recognized that its precise meaning is that 25 persons per 100,000 population did die from a given kind of accident during a year's time, and we are now perceiving that the individual chance of death was $25 \times 10^{-5} = 0.00025$ or about 1 in 4,000. If we assume, or have reason to believe, that the rate will continue unchanged into the future, then we may also assume, or believe, that individual chances will remain the same.

$$\frac{1{,}500{,}000}{200{,}000{,}000}\left(\frac{\text{injuries/year}}{\text{persons}}\right)$$

$$= 7.5 \times 10^{-3}\left(\frac{\text{injuries}}{\text{person-year}}\right)$$

The cost of injuries and property damage due to auto accidents can be similarly calculated. In this case, the recorded statistic is the total dollar value of injuries and property damage due to auto accidents for each year. This value represents the societal risk and is $15.8 billion dollars for 1971. A reasonable measure of the average individual risk is the cost per registered driver per year. For 1971, this can be computed as follows from available data:

$$\frac{\$15.8 \times 10^{9} \text{ per year}}{114 \times 10^{6} \text{ registered drivers}}$$

$$= \$140 \text{ per driver per year}$$

Historical data for risks commonly encountered by many, if not most, people in the U.S. are collected by many organizations (e.g., National Safety Council, Ref. 1, and the U.S. Government, Ref. 2), for the purposes of assessing various risks. Table 2-1 displays some selected yearly accident fatality statistics for the U.S. The data are presented in both societal form (total numbers of fatalities) and as rates (numbers of fatalities per 100,000 resident population). For most types of accidents the rate does not change much from year to year and thus the data provide reasonably realistic bases for estimating rates for several years into the future.

Table 2-2 presents the accident data for 1967 and 1968 in terms of individual risk, i.e., the probability of death per person per year. In using numbers such as those displayed in Table 2-2, all the factors associated with them, whether expressed or implied, must be known to avoid misinterpretation and misuse of the data. For example, consider the fatalities from falls, as listed in Table 2-2. A person looking at the data at the end of 1967 might have concluded that his risk, as a member of the U.S. population, of suffering a fatal fall in the next year was one chance in 10,000. Since the number 1×10^{-4} was derived from the number of fatalities counted during 1967, using it to predict future risk involves the reasonable assumption

that the rate will remain the same (in this case, it did remain the same in 1968). Another assumption involved is that all members of the U.S. population are equally exposed or susceptible to the risk. This is rarely true in human events.

A breakdown of the 1967 data on falls by age group shows that almost 3 out of 4 (73%) fatal falls involved people of age 65 and over. Thus, the risk is much smaller for persons under 65 than for persons 65 and older, and it is not 1×10^{-4} for either group as shown in Table 2-3.

The examples presented indicate that there are many factors that contribute to the quantification and evaluation of risk. The aforementioned examples of risks due to automobiles involve fatalities, injuries and property damage that can be quantified from commonly available data. The effects are principally short term ones (i.e., quickly measurable). There are undoubtedly other contributors to risks from automobiles that are not fully included in measured data. These would involve long term effects such as life shortening and decreased earning power due to injuries. Both the automobile examples and the data in Tables 2-1 thru 2-3 indicate that there are risk factors of interest both on a societal and individual basis. In addition, Table 2-3 brings the concept that risk is not always equally distributed in the population. Thus the measurement and evaluation of risk have many facets; these will be discussed more fully in later sections of this chapter.

2.2 ATTITUDES TOWARD RISK

An apparent consistency in public attitudes toward familiar risks, such as those listed in Table 2-2, has been noted by Otway and Erdmann (Ref. 3). Types of accidents with a death risk in the range of 10^{-3} per person per year to the general public are difficult to find.[1] Evidently this level of risk is generally unacceptable, and when it occurs, immediate action is taken to reduce it.

[1] Such high risks are not uncommon in some sports and in some industrial activities, when measured for the limited groups at risk (i.e., exposed to the hazards involved).

At an accidental risk level of 10^{-4} deaths per person per year, people are less inclined to concerted action but are willing to spend money to reduce the hazard. Money is spent for traffic control, fire departments and fences around dangerous areas. Safety slogans for accidents with this risk level show an element of fear (e.g., "The life you save may be your own" as applied to automobile driving).

Risks of accidental death at a level of 10^{-5} per person per year are still recognized in an active sense. Parents warn their children about the hazards of drowning, firearms, poisoning, etc., and people accept a certain amount of inconvenience to avoid risks at this level. Safety slogans have a precautionary ring: "Never swim alone"; "Keep out of the reach of children."

Accidents with a probability of death of 10^{-6} or less per person per year are apparently not of great concern to the average person. He is aware of them, but feels they will not happen to him. He may even feel that such accidents are due partly to stupidity, e.g., "Everyone knows you shouldn't stand under a tree during a lightning storm." Phrases associated with these hazards have an element of resignation: "An act of God."

The concept that the degree of public acceptance of a risk is likely to be influenced by the perception of the associated benefits is presented in Fig. 2-1 and in Reference 4. It suggests a relationship between the benefits of an activity, expressed in arbitrary units, and the acceptable risk expressed as probability of death per year per exposed person. The highest level of acceptable risks has been taken as the normal U.S. death rate from disease; the lowest level for reference is taken as the risk of death from natural events (lightning, flood, earthquakes, insect and snake bites, etc.).

One of the obvious shortcomings of the approach in Fig. 2-1 is that it does not differentiate with respect to the magnitude of the consequences of accidents. This point is illustrated by considering two accidents with significantly different frequencies and consequences. The first occurs at a rate of once per year and results in one death per accident. The risk is

$$1 \frac{\text{accident}}{\text{year}} \times 1 \frac{\text{death}}{\text{accident}} = 1 \frac{\text{death}}{\text{year}}$$

The second type has a frequency of only once in 10,000 years but results in 10,000 fatalities per event. The risk is

$$\frac{1 \text{ accident}}{10{,}000 \text{ years}} \times \frac{10{,}000 \text{ deaths}}{\text{accident}} = 1 \frac{\text{death}}{\text{year}}$$

Although each of the accidents indicated above has the same average annual risk, there is a factor of 10,000 in the size of the accidents. Society generally views the single large consequence event less favorably than the total of small events having the same average risk.

This attitude leads to the concept of "risk aversion." The term risk aversion is used to indicate, among other things, that accidents having the same average societal impact may be viewed differently depending on the sizes of the individual events. In general, single large accidents are viewed less tolerantly than multiple smaller accidents, even though the average annual consequences of the two are equal. In fact, the public appears to accept more readily a much greater societal impact from many small accidents than it does from the more severe, less frequent occurrences that have a smaller societal impact. One of the clear indications of this attitude is indicated by the public (and news media) attitude toward fatalities from automobile accidents in contrast to those from aircraft crashes. It appears that the public's aversion to large consequence events may be largely due to the view that, if such events are at all possible, they are likely, and their low probability is to be discounted.

The analyses referenced above are interesting because they represent early attempts to quantify the acceptability of the risks associated with a given activity in relation to the benefits gained from this activity; however, this field is still highly formative and much in need of development. These analyses are, therefore, of limited utility in this study. Explicit techniques for assessing the total cost of various risks and the total benefits derived from the activities causing them are still in the early stages of development even for measurable (fairly likely) risks. In the area of risks from low probability events that have not been observed, it is clearly not yet possible to perform a rigorous cost-benefit assessment. Decisions in the area of risk, as in many other areas, have generally been made on a qualitative basis with less than complete cost-benefit analyses available. Whether this approach can be improved upon in the near future is still an open question.

2.3 RISK DETERMINATION

This section briefly describes methods generally utilized for determining risks and provides a number of comments on the interpretation of numerical risk values. The discussion is divided into two parts: high probability (or likely) events and low probability (or unlikely) events. High probability events include those which have occurred frequently enough in the past to provide a basis for establishing a realistic determination of the past risk experience; i.e., their frequency and consequences have, in effect, been measured. Low probability events generally have not been observed and there is little or no overall experience on which to base the likelihood or consequences of their occurrence.

2.3.1 HIGH PROBABILITY EVENTS

The usual way of estimating risks for frequent (high probability) events is to use the data from the historical record of these events covering a suitably large segment of society. As previously indicated, there are many sources of applicable historical data and results of prior risk determinations. Examples of the results of such studies for broad categories of accidents are given in Tables 2-1 and 2-2. Normally, the available historical records provide sufficient detail to permit such broad category risks to be separated into more distinct elements that may be of special interest for a particular risk study as is indicated in Table 2-3.

The information from such risk studies is then used as a basis for estimating the risk expected in some future time period. In projecting the future risk, consideration is given to potential future influences in the risk pattern as well as the historical variation. It is well recognized that insurance companies use this procedure to determine the premium rate on policies they underwrite. They, of course, recognize that it is possible for the level of risk to change. Thus, life insurance premiums are often calculated assuming a somewhat higher fatality rate than is anticipated and if the actual experience during a given year shows the fatality rate to be less, the policy holder may receive a rebate in the form of a dividend.

2.3.2 LOW PROBABILITY EVENTS

The previous section describes how estimates of risk can be made when directly applicable accident experience data exists. However, many potential risks to which society is exposed occur at such a low frequency that they have never been observed. For example, such cases could include a large meteor falling into a city. The risks associated with such low frequency events are more difficult to estimate and express in a meaningful way than those of more frequent events.

In some cases the probability of rare occurrences can be obtained by dividing the total occurrence into a series of events for which the individual probabilities of occurrence are known. A simple example of this is the chance of getting heads every time in fifty random flips of a fair coin. From experience we know the chance of getting heads in one flip is 0.5, the chance of getting heads both times in two flips is $(0.5)^2 = 0.25$ and in fifty flips the chance is $(0.5)^{50}$, which is about one chance in 10^{15}. Thus, although this event has undoubtedly never been observed, an estimate of its probability can be achieved. Similarly the chance of getting four-of-a-kind in two successive hands in a five card stud poker game can be calculated. Analysis of poker hands has shown that the probabiliy of getting four-of-a-kind once is about one in four thousand. Thus, the chance of getting four-of-a-kind in two successive hands is about 10^{-7}. In these cases each rare occurrence was broken down into more likely events that were all the same; but this type of analysis is also applicable when the group of more likely events is of more than one type and/or frequency. The breaking up of a rare event into a series of more likely events is a basic principle of the event tree and fault tree techniques (see Chapter 4) utilized for determining probabilities of accidents in this study. Application of the above technique has involved the determination of the failure probability of systems by combining the failure probabilities of their individual parts and components.

When an unlikely event cannot be described as a sequence of more likely events, it is sometimes possible to estimate its probability by extrapolation. Suppose, for example, the highest observed level of a river at some point was 35 feet above the normal level and an estimate of the likelihood of the river reaching the 40 foot level is desired. The historical frequency of floods versus their height can be plotted and extrapolated to predict the frequency of a flood height of 40 feet. Extrapolation requires that the physical factors affecting a particular situation remain constant. Thus, while one may be able to easily estimate the likelihood of a flood level of 40 ft., given a historical level of 35 ft., it may not be valid to extrapolate to the 50 foot flood, or to the 40 foot flood that might occur 1,000 years in the future.

By using the principles previously discussed it is possible to make reasonable estimates of the probabilities of very unlikely events. Chapter 4 includes detailed descriptions of how these basic principles have been applied in this study of reactor accident risks relative to other societal risks. In addition, possible errors in these methods are identified and estimates of their magnitude are provided.

In the analysis of low probability events it is rather common to speak of the recurrence rate of an event, e.g., the 10,000 year flood, or the 10,000 year earthquake. This is another way of describing a rare flood or earthquake that has a probability of occurrence of 10^{-4}/year. Such estimates are usually extrapolations of limited experience and should not be interpreted too literally to mean the worst flood we expect in the next 10,000 years, since this would imply there would be no change in the factors (climate, local topography, etc.) affecting the frequency over the 10,000 year period. Such changes can, of course, occur in the long time periods involved. Also, just because an event is determined to have a probability of occurring only once in 10,000 years, doesn't mean that it will be 10,000 years before it occurs or that it will occur at that time. It means that the event would occur on the average of once every 10,000 years; however, although it is very unlikely, it could occur in this century.

Similar misinterpretations can easily be made with respect to the probabilities of reactor accidents. For example, suppose the probability of an accident involving melting of the nuclear core in today's reactors is 10^{-5}/reactor-year. Since about 1,000 reactors are expected to be in operation in the year 2000, there may be a tendency to say the probability of such an accident in the year 2000 will be $(10^{-5})(10^3) = 10^{-2}$. The error in this extrapolation is that it assumes the failure rate will remain constant at 10^{-5} for the next 25 years. To illustrate how inaccurate such an

extrapolation can be, consider the commercial aircraft industry which is similar at least in that it has developed with constant attention being paid to safety. Figures 2-2 and 2-3 show fatalities versus time per hundred million passenger miles and fatal accidents versus time per operation (landing or takeoff), respectively. These figures show that there was a general improvement in the safety level of commerical air travel over the time periods covered. Similar experience with motor vehicle operation is indicated in Fig. 2-4. These examples, and others, reflect the ability to take advantage of increased knowledge in order to improve safety. From this previous experience, it is not unreasonable to expect a similar learning curve for the nuclear reactor industry where increasing attention is being devoted to safety both within the AEC and in the industry as a whole.

2.4 PRESENTATION OF RISK ESTIMATES

A common problem in comparing risks in the diverse activities in which man engages is that the specific consequences of various accidents or natural events are usually difficult to express in a common unit. The consequences will usually include fatalities and injuries to people as well as damage to property. Some risk studies have attempted to handle this problem by converting all consequences into a single unit. For example, a practice generally in use for expressing occupational fatalities and non-fatal injuries together is to use lost man-days of work as a unit. In this approach a value of 6,000 man-days is usually assigned for fatalities and permanent disabilities (Ref. 5). In some studies this approach is extended by expressing fatalities and injuries to people in dollar values. This is then added to the dollar value of property damage in order to reflect the total societal cost in dollars. While such approaches are convenient, the difficulty with their use is that there is not general agreement on the value of a human life or the value to be associated with injuries that have not occurred on a large scale. Also, many people would likely view the assignment of dollar or work lost values to fatalities as being inconsistent with their personal views of this type of loss.

In view of the difficulties involved in expressing the consequences of various accidents in a common unit, this study has selected four types of consequences for the determination and comparison of accident consequences. These are:

a. Early fatalities,

b. Early illnesses,

c. Late health effects attributable to the accident,

d. Property damage.

With respect to the selection of these types, it is noted that data on the previous accident and natural event experience in the U.S. are frequently available for types a, b, and d. Further, information on type c is sometimes available in selected studies.

In this study the major types of accidents have been identified and their probability of occurrence estimated on the basis of event tree and fault tree analyses of reactor operations. Each of these accidents has been analyzed to determine the range of consequences associated with it in terms of fatalities, illness, long-term health effects, and property damage. The results of these studies provide the probability-consequence relationships which will serve as the basic information in expressing the reactor accident risks presented in Chapter 5.

Similar determinations are made for low probability high consequence non-nuclear accidents that could result from other technological undertakings. Specifically; dam failures, aircraft crashes into large concentrations of people, and the release of large amounts of chlorine, (a toxic chemical), have been studied and are compared with nuclear accidents.

To provide additional perspective on the significance of potential reactor accidents, the risks due to nuclear accidents are also compared, in Chapter 6, to the more common societal risks resulting from man's technological activities and from natural events.

References

1. Accident Facts, yearly publication of National Safety Council.

2. Statistical Abstracts of the U.S., yearly publication of U.S. Department of Commerce.

3. Otway, H. J. and Erdmann, R. C. "Reactor Siting from a Risk Viewpoint," Nuclear Engineering and Design, 13 (1970) 365-376. North-Holland Publishing Co.

4. Committee on Public Engineering Policy, National Academy of Engineering, "Perspectives on Benefit-Risk Decision-Making" report of a colloquium, April 26-27, 1971, National Academy of Engineering, Washington, D.C. 1972. References to page 1, and to paper presented by Chauncey Starr, "Benefit-Cost Studies in Sociotechnical Systems," pp. 17-42.

5. The American National Standards Institute, "The American National Standard Method of Recording and Measuring Work Injury Experience," ANSI-216.1-1967.

6. National Safety Council, "Accident Facts," 1968-71 editions, National Safety Council, 425 N. Michigan Avenue, Chicago, Illinois 60611.

7. "The Safety of Nuclear Power Reactors and Related Facilities," WASH 1250, United States Atomic Energy Commission, July 1973.

TABLE 2-1 SOME U.S. ACCIDENT DEATH STATISTICS (Ref. 6) - 1967-1970

Accident	Total Deaths				Number per 100,000 of resident population			
	1967	1968	1969	1970	1967	1968	1969	1970
Motor Vehicle	53,100	55,200	56,400	54,800	26.8	27.6	27.9	26.9
Falls	19,800	19,900	19,000	17,500	10.0	10.0	9.4	8.6
Fires, burns	7,700	7,500	7,100	6,700	3.9	3.7	3.6	3.6
Drowning	6,800	7,400	7,300	7,300	3.4	3.7	3.6	3.6
Firearms	2,800	2,600	2,600	2,300	1.4	1.3	1.3	1.1
Poisoning	2,400	2,400	2,500	3,000	1.2	1.2	1.2	1.5
Cataclysm	155	129	NA	NA	0.08	0.06	NA	NA
Lightning	110	162	NA	NA	0.06	0.08	NA	NA

NA = not yet available from this source.

TABLE 2-2 SOME U.S. ACCIDENT DEATH STATISTICS (Ref. 7) - 1967, 1968

Accident	Total Deaths		Probability of Death per Person per Year	
	1967	1968	1967	1968
Motor Vehicle	53,100	55,200	2.7×10^{-4}	2.8×10^{-4}
Falls	19,800	19,900	1.0×10^{-4}	1.0×10^{-4}
Fires, burns	7,700	7,500	3.9×10^{-5}	3.8×10^{-5}
Drowning	6,800	7,400	3.4×10^{-5}	3.7×10^{-5}
Firearms	2,800	2,600	1.4×10^{-5}	1.3×10^{-5}
Poisoning	2,400	2,400	1.2×10^{-5}	1.2×10^{-5}
Cataclysm	155	129	8×10^{-7}	6×10^{-7}
Lightning	110	162	6×10^{-7}	8×10^{-7}

TABLE 2-3 1967 FALLING DEATHS - BY AGE GROUP

Deaths by Falling 1967	Number per 100,000 in Age Group	Probability of Death per Person per Year (in age group)
19,800 total for all ages	10	1×10^{-4}
14,454 at age 65 and over	75	7.5×10^{-4}
5,346 at ages below 65	3	3×10^{-5}

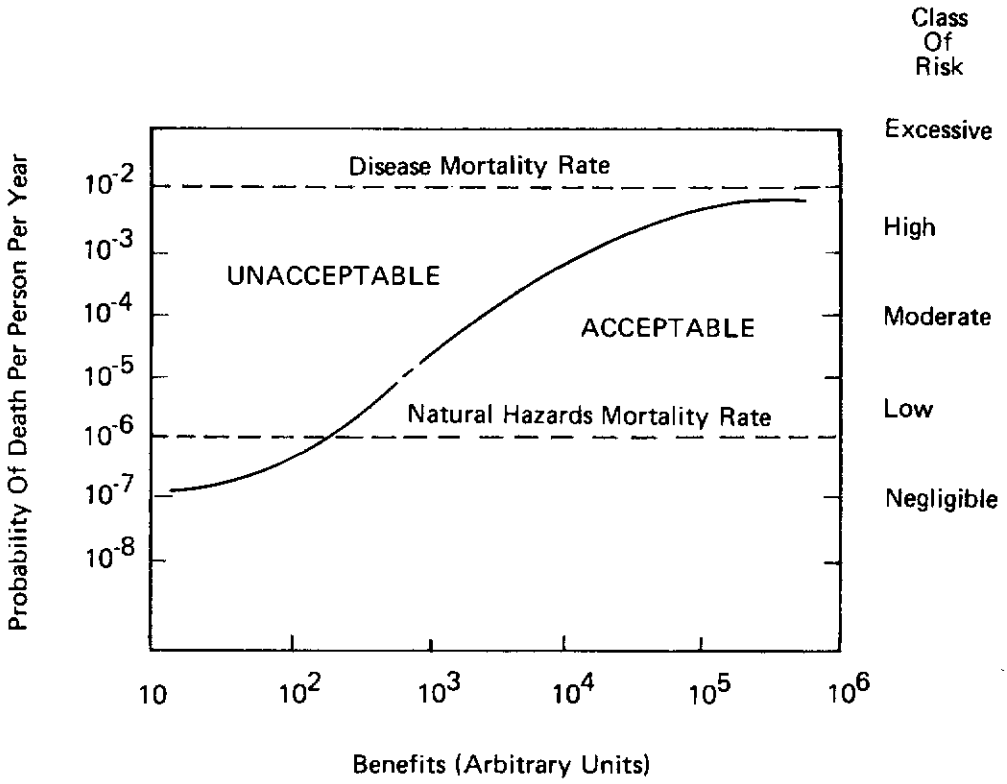


FIGURE 2-1 A Benefit-Risk Pattern

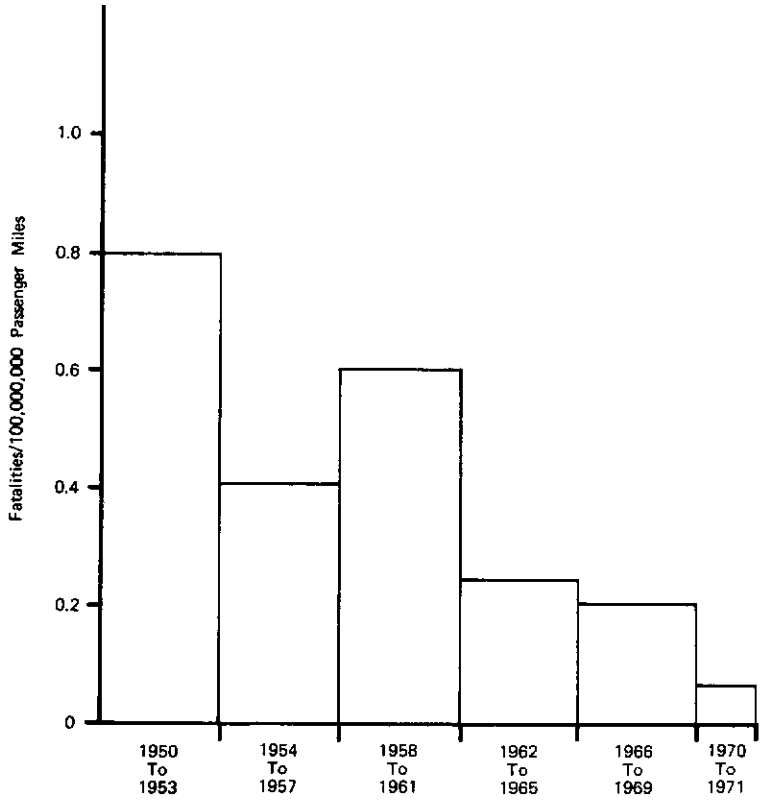


FIGURE 2-2 Fatality Rates in Commercial Air Travel [Data from Accident Facts, 1972 Edition. Covers 1950-1971.]

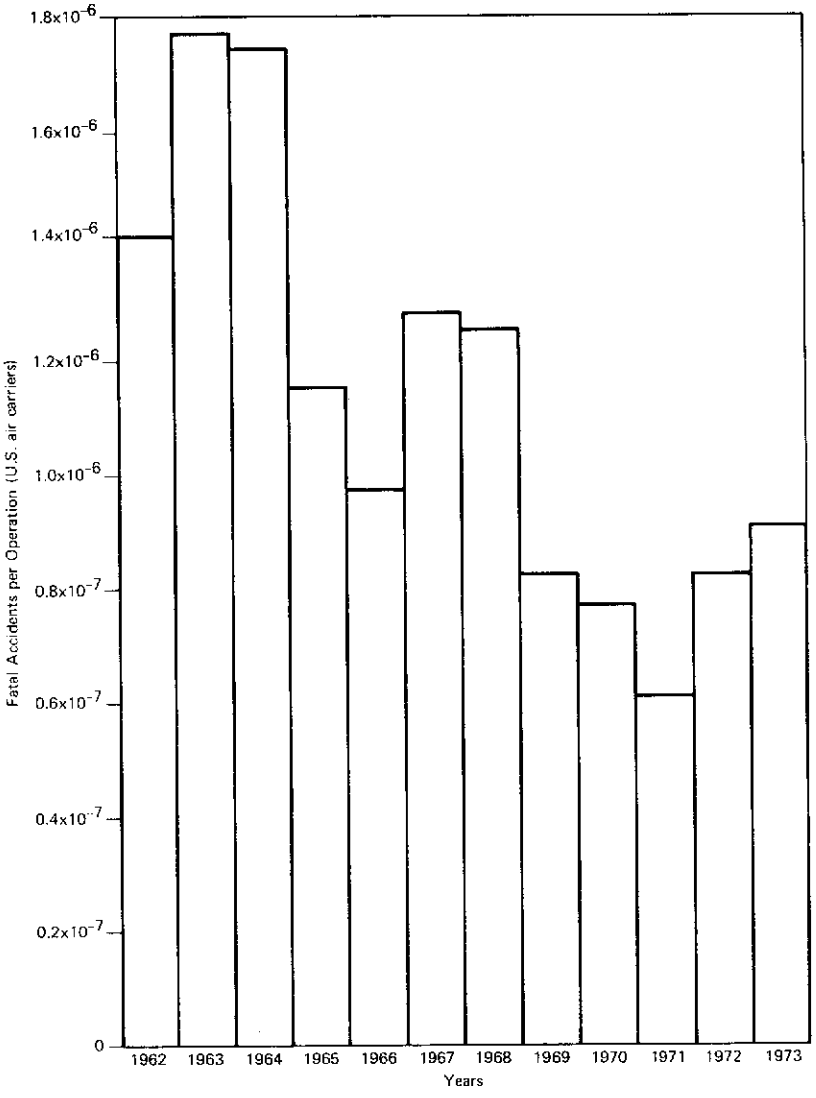


FIGURE 2-3 Fatal Accidents Per Operation (Landing or Takeoff) as a Function of Time for the U.S. Air Carrier Fleet

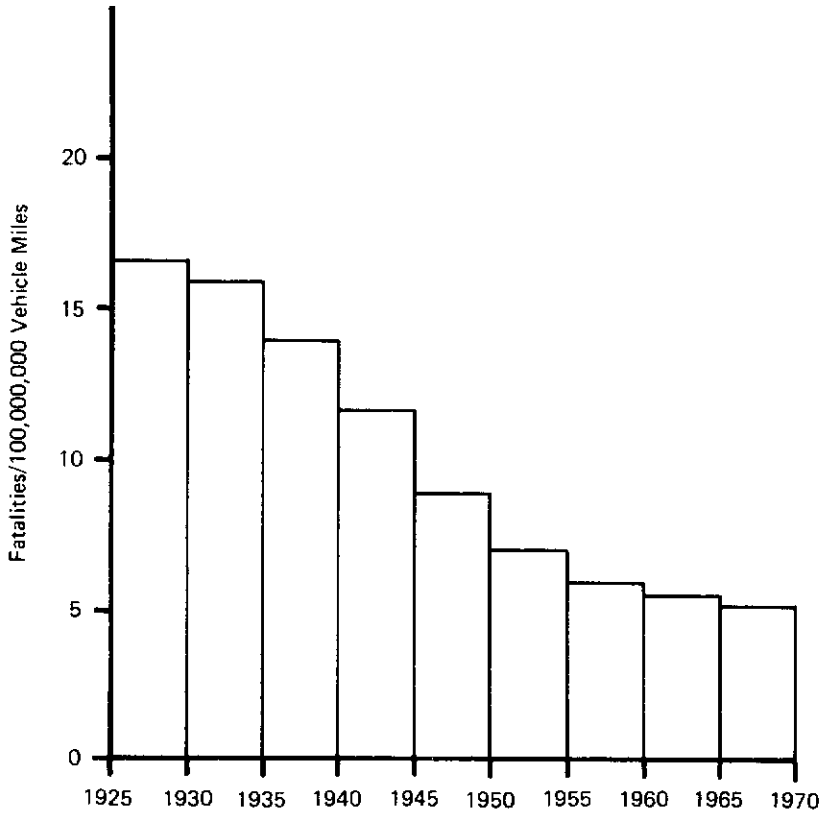


FIGURE 2-4 Fatality Rates in Motor Vehicle Travel [Based on data from Accident Facts, 1972 Edition. Covers 1925-1970.]

Chapter 3

The Nature of Nuclear Power Plant Accidents

3.1 INTRODUCTION

Nuclear power plant accidents differ from those in conventional power plants because they can potentially release significant amounts of radioactivity to the environment. While very large amounts of radioactivity are generated by the fission process in the uranium dioxide fuel in a nuclear plant, the bulk of this radioactivity (about 98%) remains in the fuel as long as the fuel is adequately cooled.[1] For large amounts of radioactivity to be released from the fuel, it must be severely overheated and essentially melt. Based on this knowledge, the major types of nuclear power plant accidents that have the potential to cause large releases of radioactivity to the environment have for some time been recognized. Attempting to prevent such accidents and to mitigate their potential consequences have been the primary objectives of nuclear power plant safety design.

The safety design approach for nuclear power plants has often been described as consisting of three levels of safety involving (1) the design for safety in normal operation, providing tolerances for system malfunctions, (2) the assumption that incidents will nonetheless occur and the inclusion of safety systems in the facility to minimize damage and protect the public, and (3) the provisions of additional safety systems to protect the public based on the analysis of very unlikely accidents. The safety design approach has also been described as involving the use of physical barriers (fuel, fuel cladding, reactor coolant system, containment building) to attempt to prevent the release of radioactivity to the environment.[2] The above descriptions are valid, but both are general statements covering the detailed concepts underlying reactor safety design. A definition of the locations and amounts of radioactivity in a nuclear power plant and an examination of the processes by which significant amounts of this radioactivity can be released from the fuel and transported to the environment outside the containment building, provides a somewhat more definitive view of the various elements that enter into reactor safety approaches.

All the places in which fuel is located in a nuclear power plant and the amount of radioactivity in each location are identifiable. This is shown in section 3.2, which indicates that by far the largest amount of radioactivity resides in the reactor core. A smaller, but still large amount of radioactivity is located in the spent fuel storage pool at the time refueling of the reactor is completed.[1] In both these locations, the fuel is subjected to heating due to absorption of energy from the decay of radioactive materials. This continues even after reactor shutdown has terminated the fission process. This decay heat can be the source of overheating in fuel in a shutdown reactor or in fuel that has been removed from the reactor. Immediately following the shutdown of a reactor that has operated about a month or longer, the decay heat amounts to about 7% of the prior operating power level. While the heat has an initial rapid decrease after reactor shutdown, it constitutes a substantial heat source for some time, and continued cooling of the fuel is required.

Overheating of fuel occurs only if the heat being generated in the fuel exceeds the rate at which it is being removed. This type of heat imbalance in the fuel

---

[1] Small amounts of radioactivity are released from the reactor fuel or are created by neutron irradiation of plant materials in normal operation. These amounts are small enough to be collected and disposed of with negligible risk as indicated in WASH-1250, Chapter 4.

[2] Appendix I, section 2 contains a discussion of the interrelationship of the various barriers.

[1] There are two other places where smaller amounts of radioactivity are located; the waste gas storage tank and the liquid waste storage tank. These are discussed in section 5 of Appendix I.

in the reactor core can occur only in the following ways:[1]

a. The occurrence of a loss of coolant event will allow the fuel to overheat (due to decay heat) unless emergency cooling water is supplied to the core.

b. Overheating of fuel can result from transient events that cause the reactor power to increase beyond the heat removal capacity of the reactor cooling system or that cause the heat removal capacity of the reactor cooling system to drop below the core heat generation rate.

Item a. indentifies a class of accidents, called loss of coolant accidents (LOCAs), in which a rupture in the reactor coolant system (RCS), would lead to a loss of the normal coolant. The rupture would allow the high pressure, high temperature RCS water to flash to steam and blow down into the containment building. To cope with this type of potential event, a set of systems called engineered safety features (ESFs) are provided in each plant. A number of the engineered safety features, as well as physical processes, act to reduce the amount of radioactivity released to the environment should either a LOCA or transient event result in a significant release of radioactivity from the reactor core. For instance, a containment building is provided to contain the radioactivity released from the fuel and to delay and reduce the magnitude of release to the environment. Some of the radioactivity would be deposited on surfaces within the containment building or would be absorbed by water sprays, water pools or filters provided for this purpose. LOCAs and ESFs are discussed briefly in section 3.3 of this chapter.

Item b. identifies a class of events called transients. A nuclear plant includes various electrical safety circuits and a system for rapid termination of the fission process to attempt to protect against damaging transients. The ESFs also serve to mitigate consequences should the transients result in severe overheating of the fuel. Transients are discussed further in section 3.4 of this chapter.

The spent fuel storage pool (SFSP) holds fuel that has been removed from the reactor and that is being stored until its heat generation rate decays to a low level at which time fuel is permitted to be shipped to a fuel reprocessing plant. The decay heat rate of the fuel in the storage pool is much lower than that of the fuel in an operating reactor core. At these low heat rates, the fuel is adequately cooled by the pool water, and significant releases of radioactivity can occur only in accidents involving essentially complete loss of water from the pool. These potential accidents are discussed in section 3.5.

For those readers not familiar with the physical features of nuclear power plants, it would be useful to refer to Appendix IX. However, a small amount of descriptive material is presented below.

The uranium dioxide fuel pellets used in current reactors are illustrated in Fig. 3-1. During normal reactor operation the bulk of the radioactivity remains trapped in the fuel pellets since the uranium dioxide, a ceramic of high melting point (~5,000°F), effectively retains the bulk of the radioactivity. A typical fuel rod is shown in Fig. 3-2. The gas plenum at the top of the fuel rod collects the small amount of gaseous radioactivity that normally leaks from the fuel pellets during operation. Figures 3-3 and 3-4 show the reactor coolant systems (RCS) for a typical PWR and a typical BWR plant, respectively. Figure 3-5 shows the BWR RCS inside the primary containment. The BWR primary containment completely encloses the RCS and is provided with a pressure suppression pool to prevent overpressurization of the containment by the initial steam release to the containment in the event of a LOCA.[1] Figure 3-6 shows the BWR RCS and primary containment located in a reactor building. This building, sometimes called a secondary containment, is not really a containment, but a confinement building that provides a path by which radioactivity that leaks from the primary containment is discharged to the environment through filters and is discharged at an elevated level. Figure 3-7 shows the PWR RCS inside a contain-

---

[1] It is possible that some interference to water flow (commonly called flow blockage) to the core of an operating reactor might cause some localized fuel melting. Such events would not lead to significant release of radioactivity to the environment as indicated in section 3 of Appendix I.

---

[1] Isolation valves are provided at suitable locations in those RCS pipes which penetrate the containment.

ment building. A system to quench the steam released in a PWR LOCA is not needed to prevent initial overpressurization because of the large volume within the containment. However, systems are provided to remove heat and reduce the pressure in the containment building and to retain radioactivity that may be released from the core. Both PWR and BWR containments are designed to have low leakage rates in order to inhibit the release of radioactivity to the environment.

3.2 LOCATION AND MAGNITUDE OF RADIOACTIVITY

The fresh uranium dioxide pellets that serve as the fuel in the PWR and BWR reactors are only slightly radioactive. However, during reactor operation the fission process produces large amounts of radioactivity in the fuel. By far, the largest fraction of the radioactivity is associated with the fission products resulting from the fission process. Some of the neutrons produced by the fission process are absorbed, to various degrees, by structural and coolant materials and thereby generate radioactivity. This radioactivity is generally referred to as induced radioactivity. The induced radioactivity is only a minute fraction of the total radioactivity that could potentially be released from the reactor in the event of a severe accident and is, therefore, not important.

While essentially all the radioactivity in the plant is initially created in the reactor core, transfer of spent fuel assemblies from the core results in considerable radioactivity being located in other parts of the plant. The radioactivity inventory second largest in amount compared to the reactor core, is located in the spent fuel storage pool (SFSP) which holds fuel that has been removed from the reactor and is awaiting shipment to an off site fuel reprocessing facility. The average number of fuel assemblies in the SFSP constitutes about half of a full reactor core loading. Radioactive fuel assemblies in the plant may also be located in the spent fuel shipping cask which holds up to about 10 fuel assemblies. The refueling transfer from the core to the SFSP involves only a single fuel assembly at a time. In addition to the above, smaller sources of radioactivity are normally present at the plant in the waste gas storage tanks (WGST) and the liquid waste storage tanks (LWST). These latter sources result, for example, from leakage of a small amount of radioactivity from the fuel rods during reactor operation, as well as radioactivity induced in impurities in the reactor cooling water. Typical magnitudes of the radioactive inventories in the above noted plant locations are shown in Table 3-1.

The values given in Table 3-1 are typical for a 1,000 megawatts electric (MWe) plant operating at 3,200 megawatts thermal (MWt).[1] In addition to the reactor power level, the plant radioactive inventory depends slightly on the length of power operation. For example, in the reactor core the total amount of radioactivity produced is directly related to the product of the power level and time at power. However, since the radioactivity decays to other isotopes, which are non-radioactive or less radioactive, an equilibrium amount of radioactivity occurs when the radioactive decay rate equals the production rate. For most of the radioactivity, equilibrium has occurred after several months of sustained operation. The reactor core radioactivity inventory shown in Table 3-1 is based on 550 days of sustained operation and represents the expected equilibrium radioactivity in an operating reactor.[2] The inventory of radioactivity in the SFSP is based on a plant that has a common SFSP serving two 1,000 MWe reactors. The average number of spent fuel assemblies stored in the SFSP is based on assumed normal unloading and shipment schedules. The radioactive inventory in the shipping cask is based on a full load of fuel in the largest shipping cask currently licensed, and the shortest decay period (150 days) allowed for fuel shipped in the container. The refueling radioactivity represents that amount in a single fuel assembly at three days after reactor shutdown. This time is typical of the earliest time after shutdown that transfer of fuel from the reactor core to the SFSP begins.

Table 3-1 clearly shows that the reactor core contains by far the largest source of radioactivity in the plant. It also

---

[1] The ratio between the electrical output and the thermal (heat) input defines the efficiency of a plant. Typical efficiencies of current nuclear power plants are about 31%. The term megawatt means one million watts.

[2] The 550 days represents about one-half of the full three year cycle that fuel assemblies remain in the core.

shows there is a relatively large inventory of radioactivity in the fuel in the SFSP and indicates that potential accidents of interest could result from melting of fuel initiated by a complete loss of water from the pool. While the spent fuel assemblies in a loaded shipping cask constitute a significant radioactive inventory, there is only a small potential for releasing a small fraction of this radioactivity in an in-plant accident.[1] The radioactivity in shipping cask fuel has decayed long enough so that air cooling alone is sufficient to preclude fuel melting. However, the fuel clad temperatures reached may become high enough to cause cladding failures and the release of the small amount of gaseous radioactivity that collects in the fuel rod gap and plenum. The postulated accident related to refueling transfer is the inadvertent lifting of a fuel assembly completely out of the water-filled refueling canal or SFSP.[2] Convective air cooling and heat radiation are also adequate to prevent fuel melting in this case, but cladding failures and a relatively small release of radioactivity (from the fuel rod gap and plenum) could result. The radioactivity in the waste gas storage tanks (WGST) and liquid waste storage tanks (LWST) are very small compared to the other sources. Accidents postulated for release of radioactivity from these tanks include tank ruptures as well as malfunctions that could involve release of the contents of the tank.

Although accidents that involve release of radioactivity from the shipping cask fuel, the refueling process, the WGST and the LWST would be troublesome, particularly to in-plant personnel, none of these could result in public consequences nearly as serious as accidents involving melting of the fuel in the reactor core or in the SFSP. Thus, although the study treats accidents involving all the radioactive sources listed in Table 3-1 (see Appendix I), the ensuing discussion in this chapter is directed at potential accidents involving fuel in the reactor core and the SFSP.

A discussion of the potential accidents covered in the study is provided in section 3 of Appendix I and in Addendum I to this report. The discussion notes the factors that were considered in attempting to ensure that the study considered all accidents of significance to the determination of public risk. The identification of all significant sources of radioactivity, the fact that a gross release of radioactivity can occur only if fuel melts, knowledge of the factors that affect heat balances in the fuel, and the fact that mechanisms that could lead to heat imbalances have been scrutinized for many years, all provide a high degree of confidence that those accidents of significance to risk have been identified.

3.3 LOSS OF COOLANT ACCIDENTS

A LOCA would result whenever the reactor coolant system (RCS) experiences a break or opening large enough so that the coolant inventory in the system could not be maintained by the normally operating makeup system. Nuclear plants include many engineered safety features (ESFs) that are provided to mitigate the consequences of such an event. A brief description of the LOCA sequence, assuming that all ESFs operate as designed, is as follows:

1. A break in the RCS would occur and the high pressure, high temperature RCS water would be rapidly discharged into the containment.

2. The emergency core cooling system (ECCS) would operate to keep the core adequately cool.

3. Any radioactivity released from the core would be largely retained in the low leakage containment building.

4. Natural deposition processes and radioactivity removal systems would remove the bulk of the released radioactivity from the containment atmosphere.

5. Heat removal systems would reduce the containment pressure, thereby reducing leakage of radioactivity to the environment.

If the ESFs were to operate as designed, the reactor core would be adequately cooled and only small consequences would

---

[1] See section 5 of Appendix I for a more complete discussion of potential shipping cask accidents.

[2] Many plants are designed in such a manner that it is physically impossible to completely withdraw a fuel assembly from the water using the normal refueling equipment. Although the study conservatively assumed that a fuel assembly could be withdrawn it made little difference to the overall risk assessment.

result. However, the potential consequences could be much larger if ESF failures were to result in overheating of the reactor core. The public impact would depend on a large number of factors which are discussed in detail in Appendices I, V and VI and Chapter 5. Some of the more significant factors are discussed in this chapter.

3.3.1 LOCA INITIATING EVENTS

There are a number of ways in which a LOCA may be initiated. The most commonly considered initiating event would be a break in the RCS piping. Piping breaks that could cause a LOCA range in size from about the equivalent of a 1/2 inch diameter hole up to the complete severance of one of the main coolant loop pipes (about 3 feet in diameter).[1]

The consequences of failure of pressure vessels (such as the reactor vessel and steam generators) have not normally been considered in the AEC's safety reviews since the high quality requirements applied in design, fabrication, and operation of these vessels have, in the past, been considered adequate to make the likelihood of failure of these vessels negligibly small. However, this study has considered both the likelihood and consequences of such failures in order to ascertain the extent to which they can potentially affect the overall risk from nuclear power plant accidents. The effects of steam generator failures and many types of reactor vessel failures as initiating events can be adequately controlled by existing ECCS systems. However, large disruptive reactor vessel failures could prevent adequate cooling of the core and can potentially cause failure of the containment building.

The specific LOCA initiating events analyzed in this study are:

a. Large pipe breaks (6" to approximately 3 feet equivalent diameter).

b. Small to intermediate pipe breaks (2" to 6" equivalent diameters).

c. Small pipe breaks (1/2" to 2" equivalent diameter).

d. Large disruptive reactor vessel ruptures.

e. Gross steam generator ruptures.

f. Ruptures between systems that interface with the RCS.

3.3.2 EFFECTS OF ENGINEERED SAFETY FEATURES

The basic purpose of the ESFs is the same for both PWR and BWR plants. However, the nature and functions of ESFs differ somewhat between PWRs and BWRs because of the differences in the plant designs. A number of the ESFs are included in a group termed the emergency core cooling system (ECCS) whose function is to provide adequate cooling of the reactor core in the event of a LOCA. Other ESFs provide rapid reactor shutdown and reduce the containment radioactivity and pressure levels that result from escape of the reactor coolant from the RCS. The following functional descriptions apply to current designs of BWR and PWR plants. More detailed descriptions of the ESFs are provided in Appendices I, II and IX.

The ESF functions are illustrated in Fig. 3-8. The primary functions they perform are as follows:

a. Reactor trip (RT)-to stop the fission process and terminate core power generation.

b. Emergency core cooling (ECC)-to cool the core, thereby keeping the release of radioactivity from the fuel into the containment at low levels.

c. Post accident radioactivity removal (PARR)-to remove radioactivity released from the core to the containment atmosphere.

d. Post accident heat removal (PAHR)-to remove decay heat from within the containment, thereby preventing overpressurization of the containment.

e. Containment integrity (CI)-to prevent radioactivity within the con-

---

[1] The maximum pipe diameter varies somewhat from plant to plant. The large pipe break is normally considered to be double-ended. This means that coolant from the RCS is expelled through both ends of the severed pipe, or the equivalent of two pipes that are about three feet in diameter.

tainment from being dispersed into the environment.[1]

The course of events following a LOCA initiating event is strongly influenced by the degree of successful operation of the various ESFs. The ways in which failures of the above functions influence the outcome of LOCAs are discussed briefly below. Section 2 of Appendix I discusses these in detail. Reactor trip (RT) is accomplished by rapid insertion of the reactor control rods. The action is initiated automatically by electrical signals generated if any of a number of key operating variables reaches a preset level. The way in which failure of the RT function affects a LOCA is complicated by a number of factors. For example, in the PWR, failure of the RT function in a large LOCA is of no immediate significance since the reactor is rapidly shut down by the loss of core moderator and ECC water contains boron to prevent return to power. However, as discussed in Appendix I, section 2, there are circumstances in which RT is required.

Emergency core cooling (ECC) involves a number of systems that deliver a supply of emergency coolant to the reactor core. Both PWR and BWR plants include high pressure systems primarily for coping with small LOCAs and low pressure systems primarily for large LOCAs. Together, these systems can fulfill the ECC requirement over a wide range of small to large pipe breaks.

Post accident radioactivity removal (PARR) is accomplished differently in the PWR than in the BWR. In the PWR, this function is performed by systems that spray water into the containment atmosphere. The water spray, which includes a chemical additive for enhancing iodine removal, washes radioactivity out of the containment atmosphere. In the BWR, this function is performed by the vapor suppression pool in the containment and a filtering system associated with the reactor building. The vapor suppression pool removes some of the radioactivity released from the core. The filtering system removes radioactivity that leaks from the containment into the reactor building before it is released at an elevated level.

Post accident heat removal (PAHR) is performed by systems that transfer heat from heated water within the containment to cold water outside the containment. The containment water that flows through the primary side of the heat exchanger is taken from the reactor building sump in the PWR and from the pressure suppression pool in the BWR. This is a particularly important function, since failure to perform this function can lead to overpressure failure of the containment and related failure of ECC systems. Containment integrity (CI) is provided by the containment features that serve to isolate the containment atmosphere from the outside environment.

It is evident, from the preceding discussions, that a large release of radioactivity from the reactor core into the containment would require violation of the barriers to the release of radioactivity provided by the fuel pellets, the fuel cladding, and the reactor coolant system. In current large power reactors, the amount of decay heat in the core is large enough so that it could, if not removed, melt all of these barriers and also melt through the bottom of the containment.[1]

In early power reactors the power level was about one tenth that of today's large reactors. It was thought that core melting in those low power reactors would not lead to melt-through of the containment. Further, since the decay heat was low enough to be readily transferred through the steel containment walls to the outside atmosphere, it could not overpressurize and fail the containment. Thus, if a LOCA were to occur, and even if the core were to melt, the low leakage containments that were provided would have permitted the release of only a small amount of radioactivity.[2]

However, as reactors grew larger, several new considerations became apparent.

---

[1] It should be noted here that the handling of post-LOCA hydrogen generation, a function currently required in the AEC licensing process, is omitted from the above list inasmuch as it has no significant impact on the overall risk assessment performed in this study. See section 2 of Appendix I.

[1] See Appendix VIII for a discussion of containment melt-through.

[2] Other mechanisms that had the potential to fail containment were not explicitly considered. These will be discussed later in this section.

The decay heat levels were now so high that the heat could not be dissipated through the containment walls. Further, in the event of accidents, concrete shielding was required around the outside of the containment to prevent overexposure of persons in the vicinity of the plant. Finally, it became likely that a molten core could melt through the thick concrete containment base into the ground. Thus, new sets of requirements came into being.

Emergency core cooling systems were needed to prevent core melting which could, in turn, cause failure of all barriers to the release of radioactivity. Systems were needed to transfer the core decay heat from the containment to the outside environment in order to prevent the heat from producing internal pressures high enough to rupture the containment. Finally, systems were needed to remove radioactivity from the containment atmosphere in order to reduce the amount that could leak from the containment into the environment.

The major goal behind these changes was to attempt to provide ESFs designed so that the failure of any single barrier would not be likely to cause the failure of any of the other barriers. For example, if the RCS were to rupture, ECC systems were installed to prevent the fuel from melting and thereby protect the integrity of the containment. Other features were added to aid this positive objective. For example, additional piping restraints and protective shields were required to lessen the likelihood of ESF damage that could result from pipe whip following a large break in the RCS. Knowledge that large natural forces such as earthquakes and tornadoes could cause multiple failures led to design requirements that attempted to reduce the likelihood of dependent failures from such causes. Appendix IX provides more detailed descriptions of the above and many more of the safety features in current nuclear plants.

The net result of the addition of ESFs in current large reactors was to reduce the likelihood of accidents that could have significant public impact. However, in making a systematic examination of the effects of failures of various significant combinations of ESFs, it was apparent that there are important interrelationships between the failure of various ESFs and either the need for, or the ability of, other ESFs to perform their functions. For instance, if in the event of a LOCA, all ESFs operate as designed and the containment were to close (i.e., isolate and become essentially leak tight), the consequences to the public would, in general, be quite small because very little radioactivity would be released from the core and much of that would be removed by containment systems provided for that purpose. However, if electric power were to fail, the likelihood of reactor trip and containment isolation would be enhanced, but the ECC, PARR and PAHR functions could not be performed. Thus, the core would melt, removal of radioactivity from the containment atmosphere would occur only by natural deposition processes, and the containment could fail due to overpressure.

Prior studies have indicated that a core meltdown in a large reactor would likely lead to failure of the containment (Ref. 1,2). Thus, a commonly held opinion regarding core melting is that such an event would result in a very serious accident with large public consequences. This is evidently one of the reasons that major safety efforts have been devoted to the prevention of core meltdown and little attention has been directed toward the examination of the potential relationships between core melting and containment integrity. This study has analyzed such relationships and has found that the containment failure modes, their timing, and the potential radioactive release depend strongly on the operability of the various ESFs. The following paragraphs indicate some general observations based on the containment failure investigations conducted in this study.

3.3.3 MOLTEN FUEL INTERACTIONS

Detailed discussions of containment integrity, as it is affected by the physical processes resulting from various ESF failures, and core melting are provided in Appendices I and VIII. Because of the difficulties involved in making precise predictions of the physical processes that accompany core melting in a LOCA, the study has not investigated the potential consequences of partial melting of reactor cores. However, it has been conservatively assumed that if conditions are such that some core melting would result, then essentially complete core melting would occur. It then follows that the core could melt through the bottom of the reactor vessel and through the thick, lower concrete structure of the containment. Melt-through of the containment would be predicted to occur about one-half to one day after the accident, thus providing considerable time for radioactive decay, washout, plateout, etc., to reduce the radioactivity in the containment atmos-

phere. Furthermore, most of the gaseous and particulate radioactivity that might be released would be discharged into the ground which acts as an efficient filter, thus significantly reducing the radioactivity released to the above-ground environment. Accidents that would follow this path are thus characterized by relatively low releases and consequences. In plants that have relatively large volume containments, the melt-through path described above would represent the most likely course of the accident.

As noted above, the melt-through path would be characterized by low atmospheric releases and consequences. Following this melt-through, there would be the possibility of ground water contamination through a long term process of leaching of radioactivity from the solidifying mass of fuel, soil, etc. An estimate of the nature and timing of the leaching processes and the potential contamination levels that could result at a point of human usage are presented in Appendix VII. The leaching and contamination processes would occur over an extended period of time (several to many years, depending on the particular radioactive species) and the potential contamination levels should not be substantially larger than the maximum permissible concentrations (MPC) (Ref. 3). The concentrations could potentially be controllable to even lower levels. Accordingly, the potential for ground water contamination therefore has been assessed to have a small contribution to the overall risk.

Containments may also fail by overpressure resulting from various noncondensible gases released within the containment as a result of core melting. These gases would arise from a number of sources. At high temperatures the zircaloy cladding of the fuel and the molten iron from support structures would react actively with water to generate large volumes of hydrogen. Also, in penetrating the bottom of the containment, the molten core decomposes the concrete, thus generating large quantities of carbon dioxide.[1] For small containments, the pressure due to the combination of these two gases would represent the most likely path to containment failure. Even though such failures would most likely occur in the above ground portion of the containment, this would take several hours from the time of core melt. Thus, there would be considerable time available for reducing the amount of radioactivity released due to decay, plateout, etc. It is not expected that large containments would be failed by this means.

At two key stages in the course of a potential core meltdown there would be conditions which would have the potential to result in a steam explosion that could rupture the reactor vessel and/or the containment.[1] These conditions may occur when molten fuel would fall from the core region into water at the bottom of the reactor vessel or when it would melt through the bottom of the reactor vessel and fall into water in the bottom of the containment. It is predicted (see Appendix VIII) that if such an explosion were to occur in the reactor vessel, it may be energetic enough to change the course of the accident. For reactors enclosed in relatively large volume containments, it is considered improbable that a steam explosion outside the reactor vessel would rupture the containment. If a steam explosion were to occur within the reactor vessel, it is considered possible that both large and small containments could be penetrated by a large missile. Such occurrences might release substantial amounts of radioactivity to the environment. However, these modes of containment failure are predicted to have low probabilities of occurrence.

3.4 REACTOR TRANSIENTS

In general, the term reactor transient applies to any significant deviation from the normal operating value of any of the key reactor operating parameters. More specifically, transient events can be assumed to include all those situations (except for LOCA, which is treated separately) which could lead to fuel heat imbalances. When viewed in this way, transients cover the reactor in its shutdown condition as well as in its various operating conditions. The shutdown condition is important in the consideration of transients because many transient conditions result in shutdown

---

[1] This is true only for concrete which contains limestone. It is not applicable to basaltic concrete.

[1] The term steam explosion refers to a phenomenon in which the fuel would have to be in finely divided form and intimately mixed with water so that its thermal energy could be efficiently and rapidly deposited in the water thus creating a large amount of steam.

of the reactor and decay heat removal systems are needed to prevent fuel heat imbalances due to core decay heat.

Transients may occur as a consequence of an operator error or the malfunction or failure of equipment. Many transients are handled by the reactor control system, which would return the reactor to its normal operating condition. Others would be beyond the capability of the reactor control system and require reactor shutdown by the reactor protection system (RPS) in order to avoid damage to the reactor fuel.

In safety analyses, the principal areas of interest are increases in reactor core power (heat generation), decreases in coolant flow (heat removal) and reactor coolant system (RCS) pressure increases. Any of these could potentially result from a malfunction or failure, and they represent a potential for damage to the reactor core and/or the pressure boundary of the RCS. In this study the analysis of reactor transients has been directed at identifying those malfunctions or failures that can cause core melting or rupture of the RCS pressure boundary. Regardless of the way in which transients might cause core melting, the consequences are essentially the same; that is, the molten core would be inside an intact containment and would follow the same course of events as a molten core that might result from a LOCA. This fact greatly simplified the determination of the transient contribution to the risk since it permitted the elimination of many transients from the risk determination solely on the basis of their relatively low probabilities compared to those of other transients.

In this study each potential transient is assessed to fall into either one of two general categories, the anticipated (likely) transients and the unanticipated (unlikely) transients. The large majority of potential transients are those that have become commonly known as anticipated transients. There are currently about 10 such occurrences per year at each nuclear power plant, including a few planned shutdowns. Some of the individual types of events, such as loss of offsite power, that contribute to this total number are relatively less likely to occur. All other transients are considered to fall into the unanticipated transient category. As shown in section 4.3, Appendix I, the relatively low probability (unanticipated) transients can be eliminated from the risk determination since their potential contribution to the risk is small compared to that of the more likely (anticipated) transients that produce the same consequence. Similar considerations of the relative probabilities permit elimination of most of the anticipated transients from the risk determination. The transients that were found to be important to the risk assessment are identified in section 4.3, Appendix V. These are the anticipated (likely) transients that involve the loss of offsite power and loss of plant heat removal systems.

3.5 ACCIDENTS INVOLVING THE SPENT FUEL STORAGE POOL

In section 3.2 the spent fuel storage pool (SFSP) is identified as having a significant radioactivity inventory, second in amount to the reactor core. Further, the decay heat levels in freshly unloaded fuel assemblies that may be stored in the pool may be sufficiently high to cause fuel melting if the water is completely drained from the SFSP. Because the maximum amount of fuel stored in the pool immediately after refueling is smaller than that in the core and because it has had time (72 hours minimum) for radioactive decay, it is a less intense heat source than a reactor core (about one-sixth) and therefore melt-through of the bottom structure of the pool would occur at a much lower rate and, in fact, may not occur at all. On the average, fuel in the pool will have undergone about 125 days of decay, and it is questionable that such fuel would melt. However, to assure that the risk would not be underestimated, it has been assumed that even this fuel would melt.

Although the pool is not within a containment building, filters in the SFSP building ventilation system and natural deposition of radioactivity within the building both aid in reducing the amount of radioactivity that might be released to the environment in the event of a spent fuel accident.

The analyses of accidents that could potentially lead to loss of fuel cooling in the SFSP are discussed in section 5 of Appendix I. The most probable ways in which such accidents could occur have been determined to be the loss of the pool cooling system or the perforation of the bottom of the pool. The latter could occur, for example, by dropping a shipping cask in the pool or on the top

edge of the pool. Both this type of accident and the loss of cooling capability, are of low likelihood. The loss of cooling capability, which has been determined to be somewhat more probable, requires that a number of audible alarms be inoperative or ignored and that the visual observation be so lax as to permit the lowering of the pool water level to continue uncorrected for about two weeks -- the approximate time required to boil off the SFSP water if cooling capability is lost. Chapter 5 will show that the size of such potential accidents are smaller than those that could involve the core.

References

1. Ergen, W. K., et al., "Emergency Core Cooling, Report of Advisory Task Force on Emergency Core Cooling," 1967, USAEC.

2. Morrison, D. L., et al., "An Evaluation of the Applicability of Existing Data to the Analytical Description of a Nuclear-Reactor Accident Core Meltdown Evaluation," Battelle Columbus Labs., BMI 1910, July 1971.

3. Code of Federal Regulations, 10CFR, Part 20.

TABLE 3-1 TYPICAL RADIOACTIVITY INVENTORY FOR A 1000 MWe NUCLEAR POWER REACTOR

Location	Total Inventory (Curies)			Fraction of Core Inventory		
	Fuel	Gap	Total	Fuel	Gap	Total
Core[a]	8.0×10^{9}	1.4×10^{8}	8.1×10^{9}	9.8×10^{-1}	1.8×10^{-2}	1
Spent Fuel Storage Pool (Max.)[b]	1.3×10^{9}	1.3×10^{7}	1.3×10^{9}	1.6×10^{-1}	1.6×10^{-3}	1.6×10^{-1}
Spent Fuel Storage Pool (Avg.)[c]	3.6×10^{8}	3.8×10^{6}	3.6×10^{8}	4.5×10^{-2}	4.8×10^{-4}	4.5×10^{-2}
Shipping Cask[d]	2.2×10^{7}	3.1×10^{5}	2.2×10^{7}	2.7×10^{-3}	3.8×10^{-5}	2.7×10^{-3}
Refueling[e]	2.2×10^{7}	2×10^{5}	2.2×10^{7}	2.7×10^{-3}	2.5×10^{-5}	2.7×10^{-3}
Waste Gas Storage Tank	-	-	9.3×10^{4}	-	-	1.2×10^{-5}
Liquid Waste Storage Tank	-	-	9.5×10^{1}	-	-	1.2×10^{-8}

(a) Core inventory based on activity 1/2 hour after shutdown.

(b) Inventory of 2/3 core loading; 1/3 core with three day decay and 1/3 core with 150 day decay.

(c) Inventory of 1/2 core loading; 1/6 core with 150 day decay and 1/3 core with 60 day decay.

(d) Inventory based on 7 PWR or 17 BWR fuel assemblies with 150 day decay.

(e) Inventory for one fuel assembly with three day decay.

FIGURE 3-1 Uranium Dioxide Pellets Used for Commercial Water Cooled Nuclear Power Plants

Typical Fuel Data

	PWR	BWR
Overall length, in.	149.7	∿164
Outside diam., in.	0.422	0.563
Metal wall thickness, in.	0.0243	0.037
Pellet diam., in.	0.366	0.477
Pellet length, in.	0.600	0.5
Pellet stack height, in.	144	144
Plenum length, in.	4.3	16
Fuel rods in fuel assembly	204	49
Fuel rod pitch, in.	0.563	0.738
Fuel assemblies in core	193	764

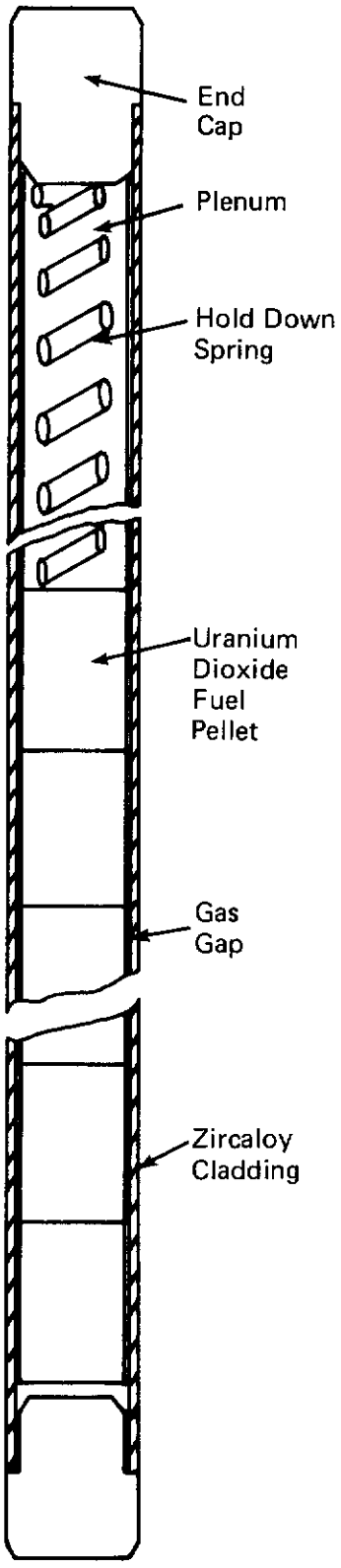


FIGURE 3-2 Cutaway of Fuel Rod Used for Commercial Water Cooled Nuclear Power Plants

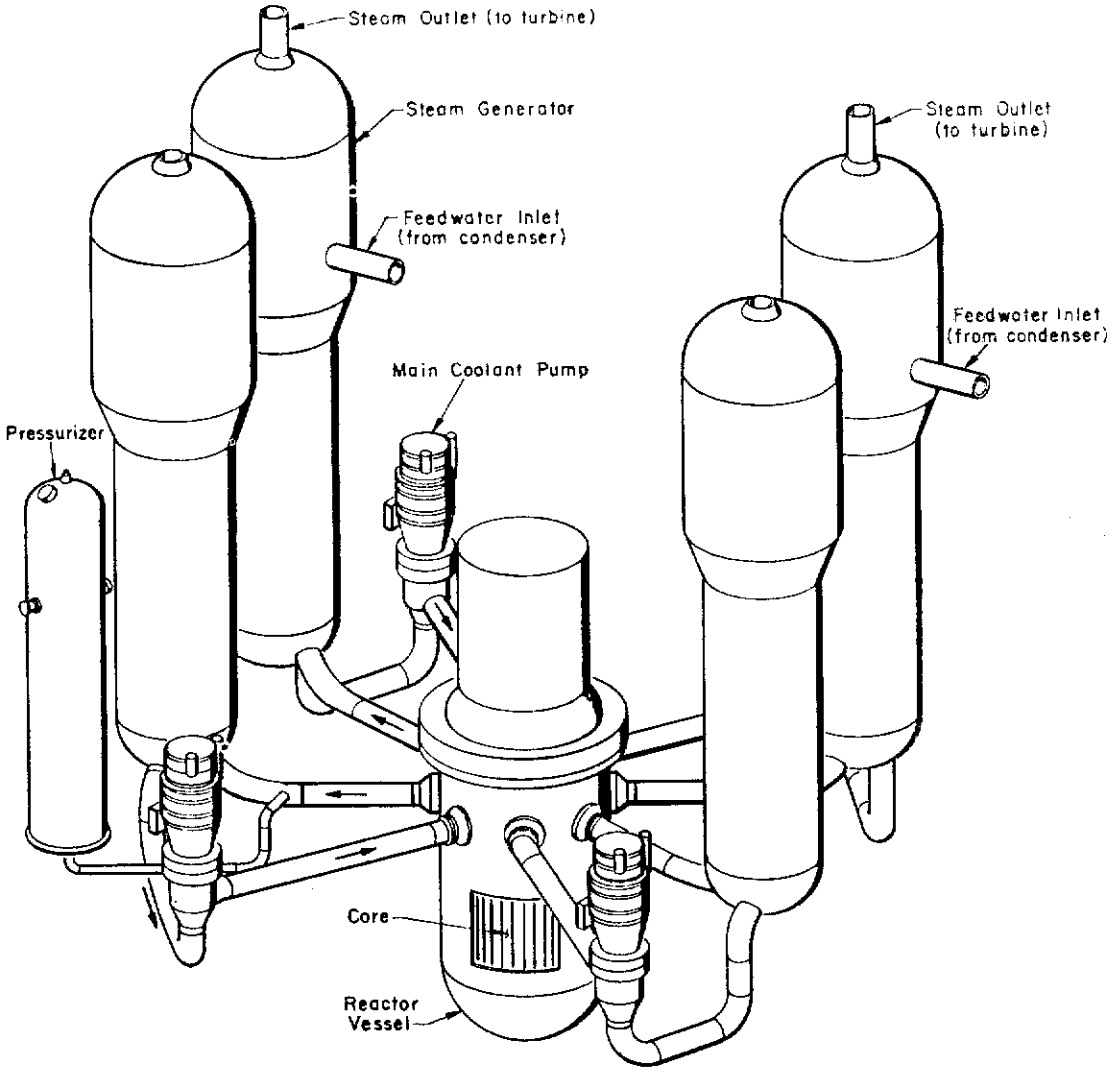


FIGURE 3-3 Schematic of Reactor Coolant System for PWR

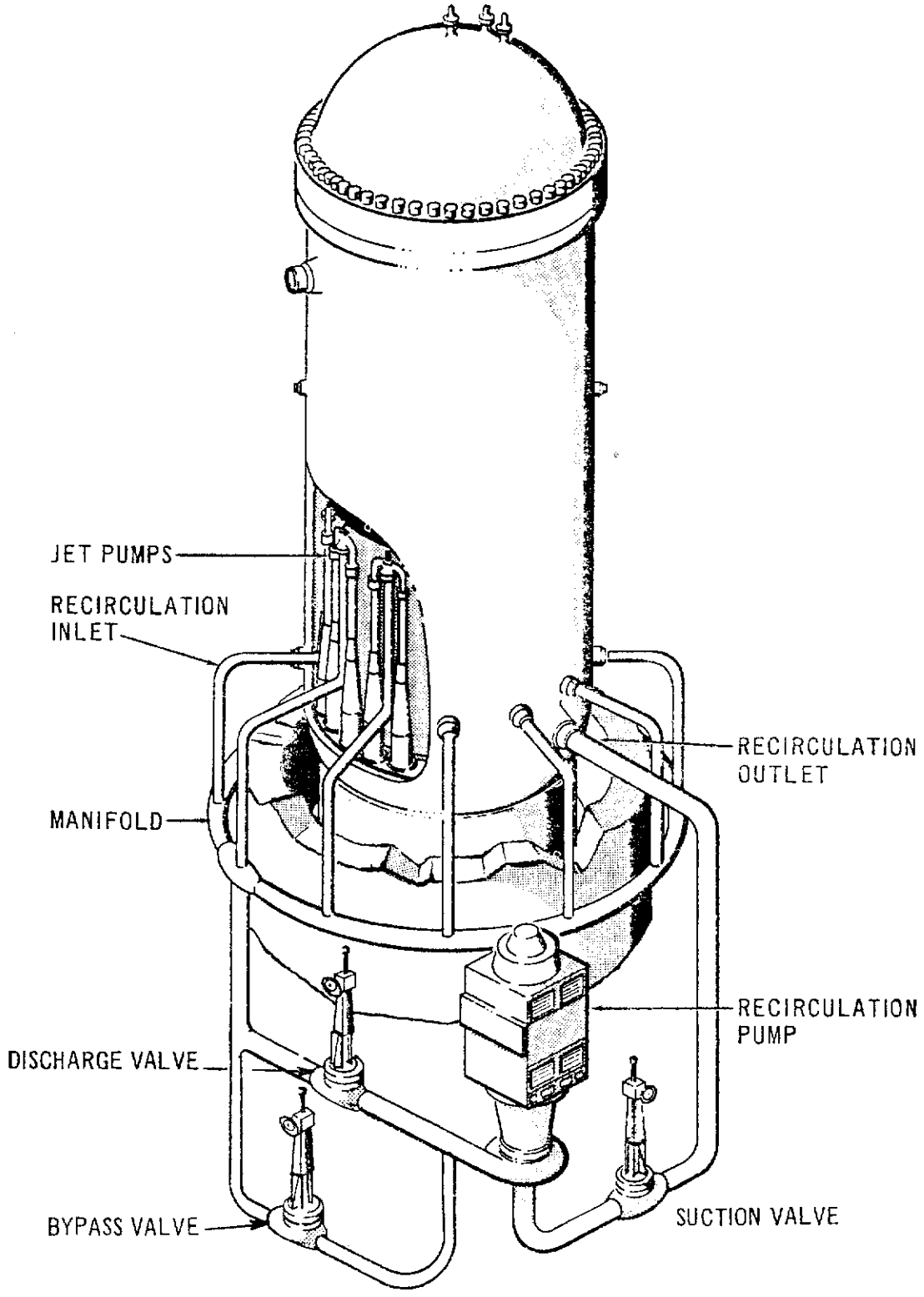


FIGURE 3-4 Schematic of BWR Reactor Coolant System

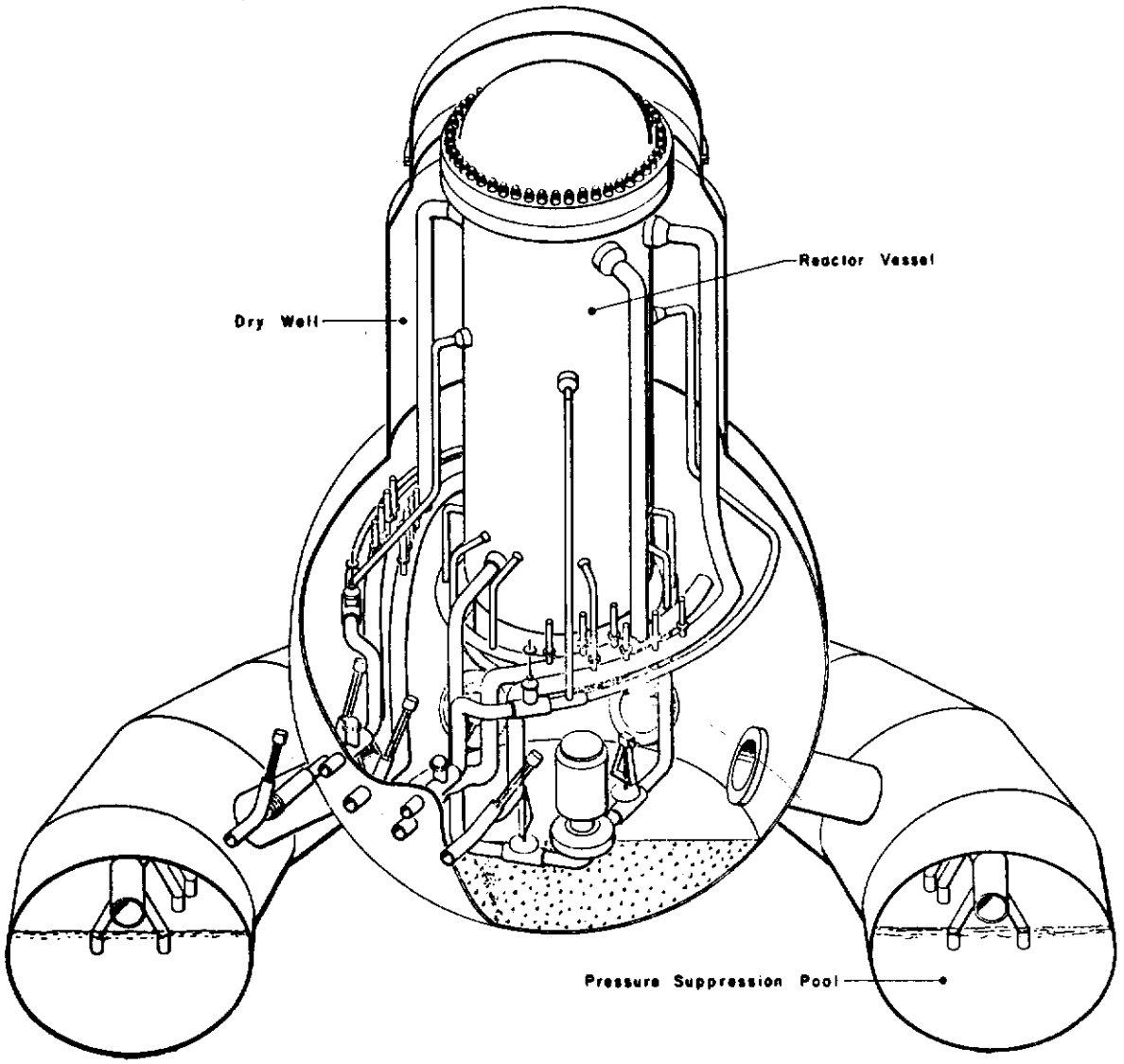


FIGURE 3-5 Schematic of Reactor Coolant System for BWR - Inside of the Primary Containment

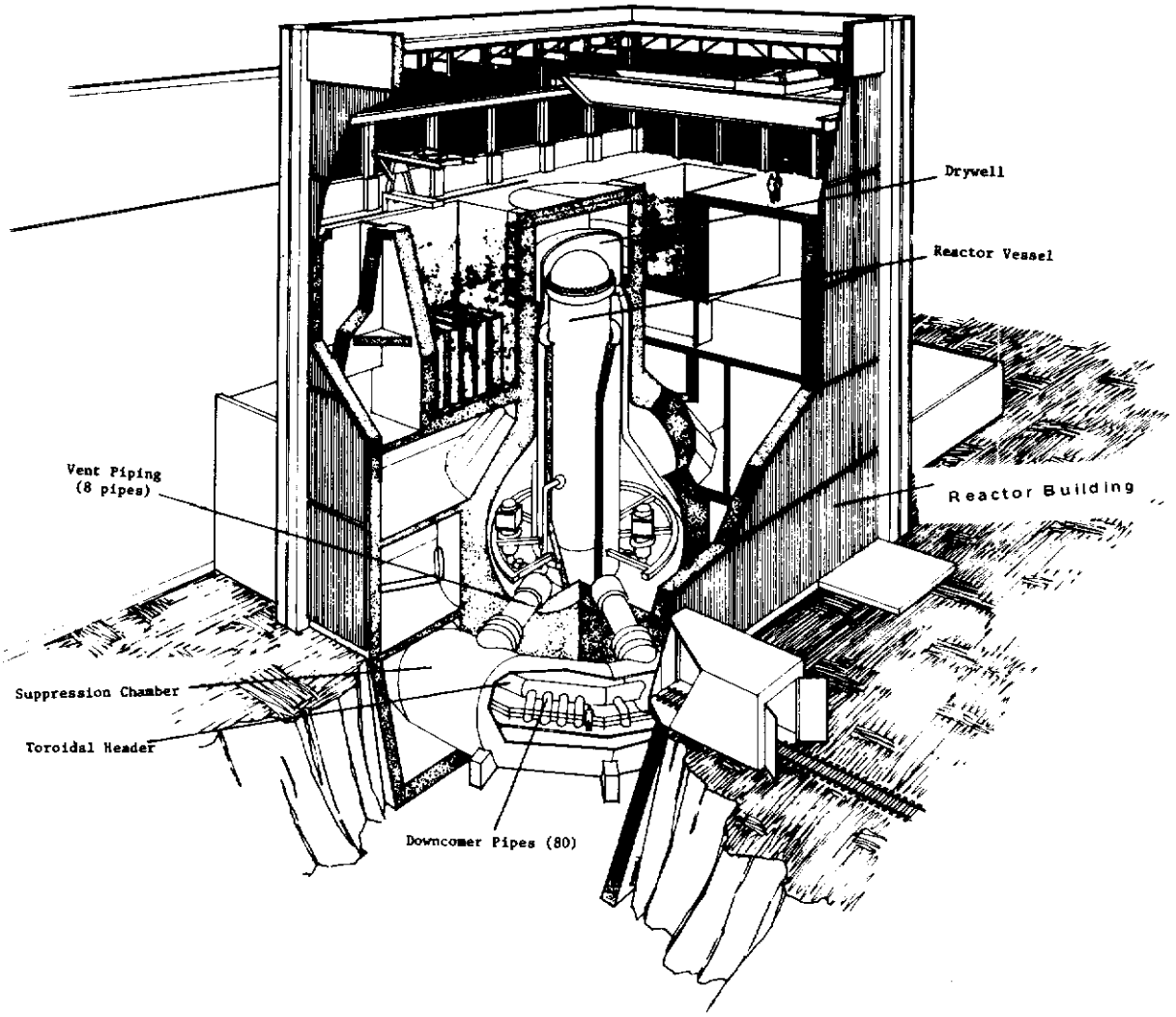


FIGURE 3-6 BWR Reactor Building Showing Primary Containment System Enclosed

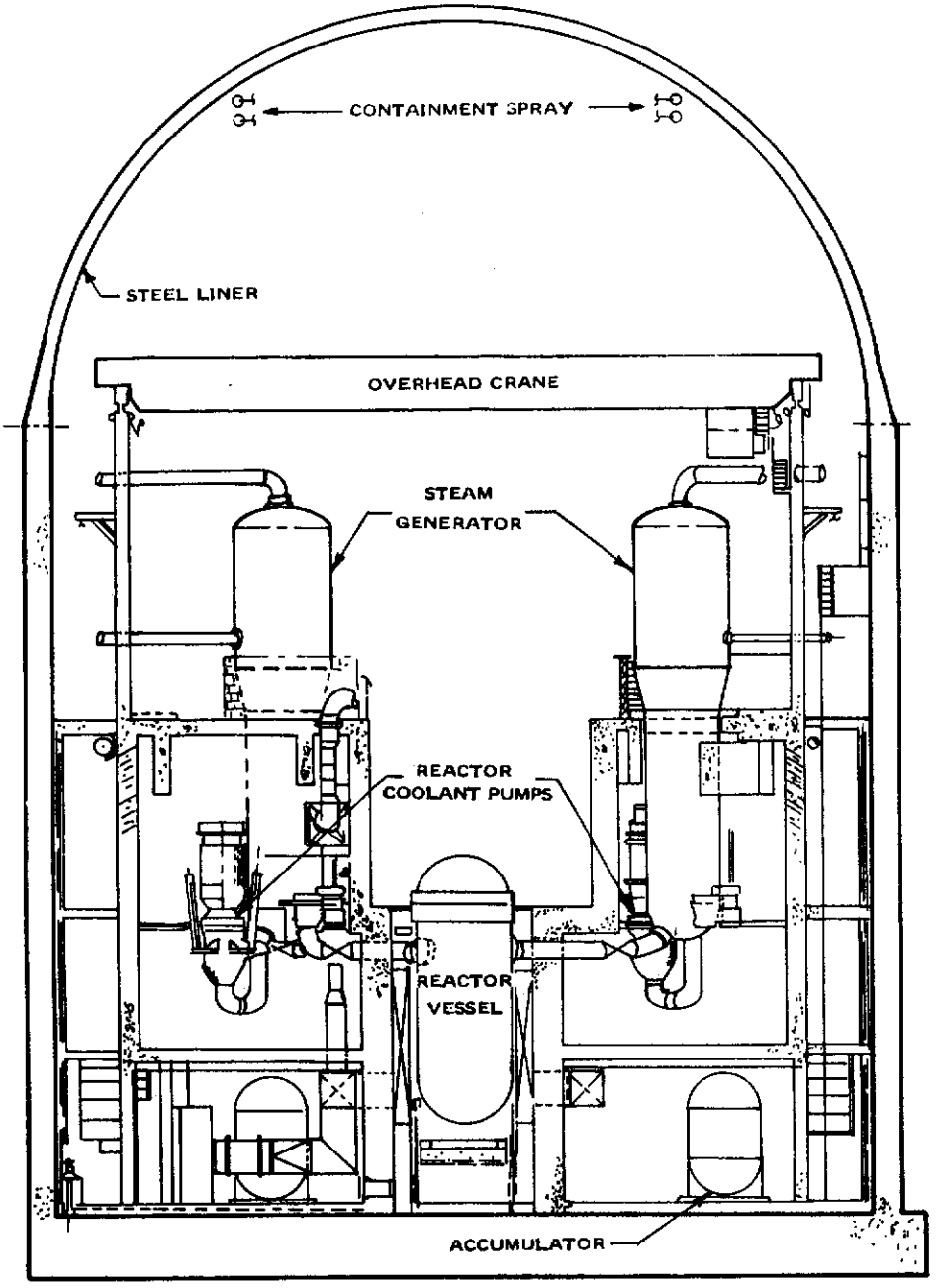


FIGURE 3-7 Typical PWR Containment

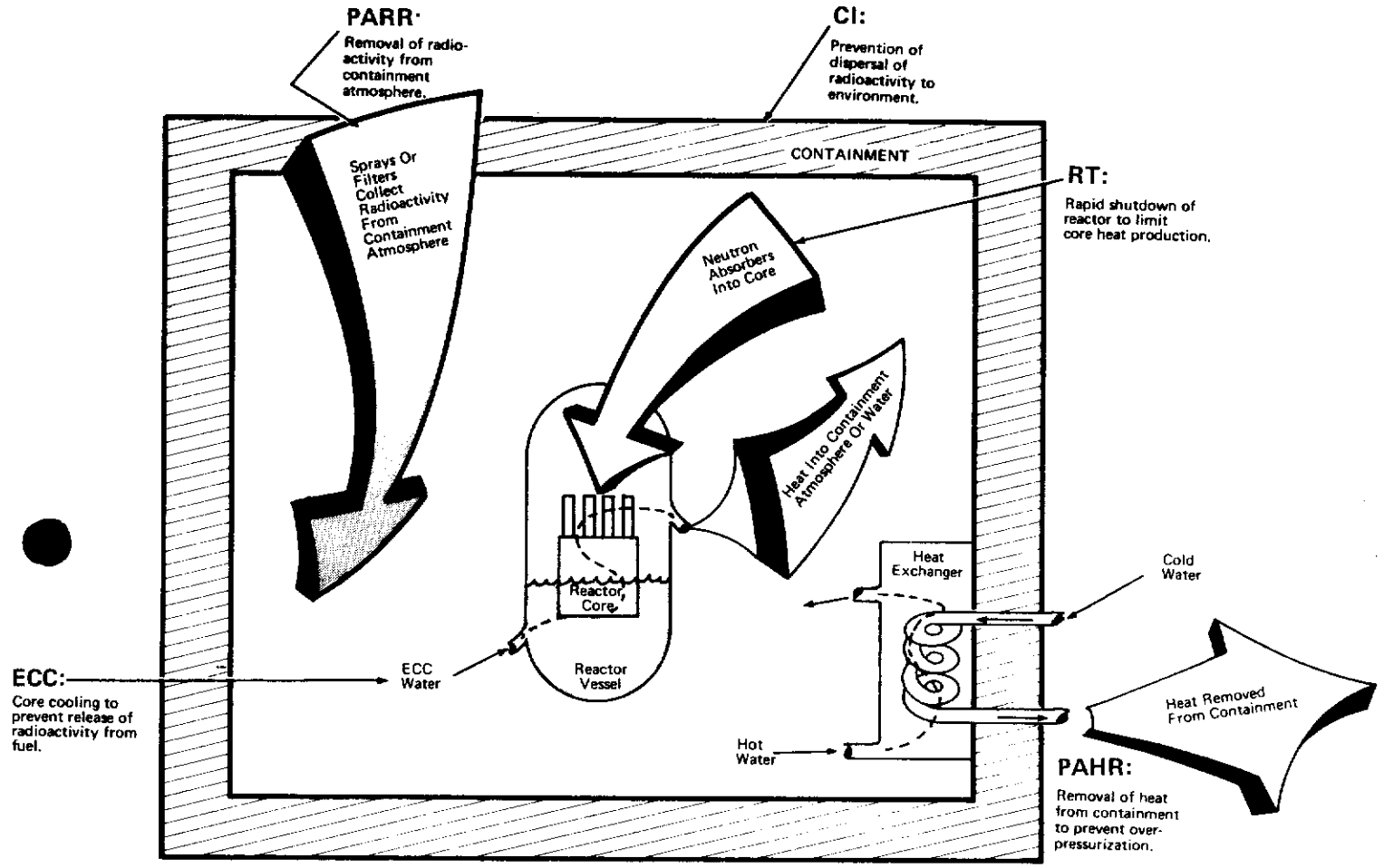


FIGURE 3-8 Power Water Reactor Loss of Coolant Accident (LOCA) Engineered Safety Feature (ESF) Functions

Chapter 4

Risk Assessment Methodology

4.1 INTRODUCTION

This study has divided the work into a number of tasks whose results were combined to produce the overall risk assessment. The detailed technical work of each task is reported in the appendices of this report. This chapter describes the methods used in each task and the way the results of each were combined to produce the final result. This discussion is brief; however Addendum I to this report provides a detailed overview of the entire methodology used.

The risk determination was divided into the three major tasks shown in Fig. 4-1.

Task I includes the identification of potential accidents and the quantification of both the probability and magnitude of the associated radioactive releases to the environment. The major part of the work of the study was devoted to this task. The organization of the work and the methodology used are discussed in section 4.2.

Task II uses the radioactive source term defined in Task I and calculates how the radioactivity is distributed in the environment and what effects it has on public health and property. The methodology used is described in section 4.3.

Task III combines the consequences calculated in Task II, weighted by their respective probabilities to produce the overall risk from potential nuclear accidents. To give some perspective to these results, they are compared to a variety of non-nuclear risks. The task is described in section 4.4.

4.2 QUANTIFICATION OF RADIOACTIVE RELEASES

The objective of this task is to generate a histogram, of the form shown in Fig. 4-2, which shows the probability and magnitude of the various accidental radioactive releases. The isotopic composition,[1] elevation of the release point above ground level and the timing and energy content associated with the release must also be determined to permit the calculation of consequences due to the releases.

This histogram could be determined for a single type of accident (such as a loss of coolant accident). By combining many accidents one can obtain a composite histogram for all important contributors. Since the histogram could be different for the various isotopes released, a full characterization of all accidents could involve a large number of such histograms. A significant effort was devoted to combining all isotopes and accidents into a single histogram for each reactor. This work is described in Appendix V.

To generate a composite histogram of the type shown in Fig. 4-2, the methodology employed must in principle be able to identify the accidents that can produce significant releases and determine their probability. To do this for all accidents in a system as complicated as a nuclear power plant is a formidable task because of the very large number of accidents that can be imagined. The problem becomes more manageable, however, when it is realized that, of this large number of potential events, many have trivial releases, many are illogical (i.e., violate known physical conditions) and others have very small probabilities compared to accidents which result in essentially the same release magnitude. To ensure that unnecessary analyses are not pursued, the methods used must provide a way for logically eliminating accidents that do not significantly contribute to the radioactive source term.

The characterization of the radioactive releases was divided into the subtasks shown in Fig. 4-3, which also indicates the report appendix applicable to each subtask. The logic for selecting the initiating events is discussed in Chapter 3. A logic diagram called an event tree was developed for those initiating events that involved complex interactions.[1] The event tree defined

---

[1] Tasks I and II consider 54 isotopes in calculating releases and consequences as indicated in Appendix VI.

[1] Event trees will be described further herein. They are also described in considerable detail in Appendix I.

the possible sequences of events subsequent to the initiating event and resulted in the definition of a number of possible accident sequences, many of which produce core melt. These systematically defined core melt sequences provided a basis for analyzing the physical processes occurring during core melt and for determining the containment failure modes and the timing of various other events (Appendix VIII). This information allowed completion of the definition of accident sequences. These completed sequence definitions then permitted, on the basis of experimental data, estimates of the amount of radioactivity that would be released from the fuel (Appendix VII). These releases, the containment failure modes, and the timing of various events provided input to a computer code called CORRAL which calculates the amounts of the various types of radioactivity released to the environment (Appendices V and VII).

To obtain the probability of a given release, it was necessary to determine the probabilities of various accident sequences identified in the event trees. These probabilities were generally obtained through the use of fault tree analysis (discussed herein and in Appendix II). Fault tree analysis produces a logic diagram to which failure rates, appropriate time intervals, and other values can be assigned and combined to derive system failure probabilities. Since the failure rate assigned to system components usually assumed that the equipment was properly designed and qualified for those aspects of nuclear service that are unique, a check was made on a selected number of components, systems, and structures to verify that such requirements had been adequately met.[1] This effort was called the design adequacy task and is described in Appendix X.

A key step in the development of system failure probabilities is gaining an understanding of any dependencies between failures. Such dependencies, known as common mode failures, are known to exist in and between the systems modeled in the fault trees and the event trees. Considerable effort was expended in identifying such dependencies and accounting for their effects.

[1]Component failure rates were also modified when the components experienced accident environments, which is described in Appendix III.

It should be recognized that the steps indicated in Fig. 4-3 do not flow as simply as implied by the sketch. For example, it was often not obvious which accident sequences were important and which made only neglibible contributions to risk. Thus, many sequences were analyzed under a set of pessimistic, simplifying assumptions. Those that showed up as significant contributors were then reanalyzed using more detailed, realistic methods. A number of such iterations were often necessary to determine the accident sequences that were the dominant contributors to the probability of occurrence of various consequences.

The event tree and fault tree methods described below are used to show relationships between component and system failure probabilities as well as interactions between various systems. The implementation of these methods often requires knowledge about the details of plant construction. Thus, for that part of the analysis requiring this detailed information, the study has used, as indicated in Chapter I, a particular PWR and a particular BWR as typical of each of these classes of plants.

4.2.1 DEFINITION OF ACCIDENT SEQUENCES - EVENT TREES

A major element in the characterization of the radioactive releases associated with potential nuclear power plant accidents is the identification of the accident sequences that can potentially influence the public's risk from such accidents. The study employed event tree methodology as the principal means for identification of the significant accident sequences.

An event tree is a logic method for identifying the various possible outcomes of a given event which is called the initiating event. The number of possible final outcomes depends upon the various options that are applicable following the initiating event. This technique has been used widely in business where the initiating event is a particular business decision and the various outcomes depend upon subsequent decisions. In business applications the trees are known as decision trees (Ref. 1). In the application to reactor safety studies the initiating event is generally a system failure and the subsequent events are, for the most part, determined by system characteristics and engineering data. In this study the trees are called event trees, and a particular sequence from the initiating

event to a final outcome is termed an accident sequence.

In this study the application of event trees was limited to the analysis of potential accidents involving the reactor core. For this purpose it was found convenient to separate the event trees into two types of trees. The first was used to determine how potential accidents were affected by failures in major systems, particularly the engineered safety systems. They cover the significant LOCA and transient initiating events.

These trees were supplemented with a second type of tree, the containment event tree, to provide combined accident sequences from the initiating event to release of radioactivity from the containment. This procedure is described briefly below and in greater detail in Appendix I and Addendum I to this report. It produced a list of systematically defined sequences leading to the release of radioactivity to the environment. The list of these accident sequences is found in Appendix V. The starting point for the development of an event tree is the event (failure) that initiates a potential accident situation. The initiating event is basically either a reactor coolant system rupture that results in a LOCA or any of a number of reactor transients. The initiating events of particular significance have been discussed briefly in the Chapter 3 sections treating LOCAs and reactor transients. Appendix I provides more detailed information on the selection of initiating events for the development of the system event trees and on the development of event trees for use in the study.

The application of event trees in determining system operability effects on potential accident sequences is illustrated by the following simplified example in which the initiating event is a large pipe break in the primary system of a reactor. The first step in developing this event tree is to determine which systems might affect the subsequent course of events. In this example these are station electric power, the emergency core cooling system, the radioactivity removal system, and the containment system. Through a knowledge of these systems it is possible to order them in the time sequence in which they influence the course of events. They are ordered in this way across the top of Fig. 4-4 which shows event trees in which the upper branch represents success and the lower branch represents failure of the system to fulfill its function. In the absence of other constraints there are $2^{(n-1)}$ accident sequences, where n is the number of headings (functions, systems, etc.) included on the tree. However, there are known relationships (constraints) between system functions. For example, if station electric power fails none of the other systems can operate because they depend upon power. In addition to such functional relations there may also be hardware common to more than one system. Once these functional and hardware relationships are incorporated, many of the chains shown in the upper tree of Fig. 4-4 can be eliminated because they represent illogical sequences. Such sequences are eliminated in the lower tree shown in Fig. 4-4. Note that elimination of the choices following failure of electric power reduces the number of sequences by about half.

The probability of failure of each system is indicated by the P values noted in Fig. 4-4. The probability of success is (1-P) since it is assumed that a system operates successfully if it does not not fail. If the events (failures, successes) are independent then the probability of occurrence of a given sequence is the product of the probabilities of the individual events in that sequence, as indicated in Fig. 4-4. Since the failure probabilities are almost always 0.1 or less it is common practice to approximate $(1-P) \approx 1$, as shown in Fig. 4-4. The probability of occurrence of each system failure is shown to be different in each accident sequence in which it appears. This is done to account for the differences in system failure probabilities that may occur due to the differing dependencies in each accident sequence.

It should be noted that as indicated by Fig. 4-4, the study developed event trees in which each branch point provides only two options, system success or system failure. No consideration is given to the fact that partial system success may occur within an accident sequence. Thus, an accident sequence is conservatively assumed to lead only to total core melt or no core melt, but never to partial core melt. This has been done because uncertainties in the calculational methods preclude predictions of the detailed conditions that lead to a partial core melt. Similarly, because of the difficulty in calculating, with reasonable certainty, the effects of partial system failure, the study has treated all such questionable cases of system operability as complete system failures. Since most applicable

systems involve considerable redundancy, the basic procedure involved determination of the fraction of the redundant equipment that must be operable to assure successful function of a particular system. The probability of failure of the system is the probability that the system is in a condition with less than this fraction of the equipment operating. This success/failure treatment can significantly affect the overall risk assessment only through accident sequences which are important contributors to risk. Since a large fraction of the sequences analyzed were found to have an insignificant effect on the risk, the fact that their analysis was done conservatively has a negligible effect on the magnitude of the total estimated risk. Those accident sequences that were found to contribute importantly to the risk were subjected to further analysis in an attempt to remove any unwarranted conservatisms.

If the event tree has been constructed with detailed information, the series of events in each accident sequence would be well enough defined so that it is possible to calculate the consequences for that particular series of events. For example, the bottom sequence in Fig. 4-4, where no core cooling would be available, can be shown to result in melting of the core and the fraction of core radioactivity that would be released can be calculated. Since, as pointed out in Chapter 3, the molten core would violate the containment, the accident could produce a release of radioactivity outside of the containment. The mode of containment failure would affect the overall probability of the sequences as well as the magnitude of the release. The event tree therefore provides a definition of the possible accident sequences from which the radioactive releases to the environment can be calculated and, if the failure probabilities are known, the probability of each release can also be calculated. Again, it should be noted that this example is greatly simplified for illustrative purposes; the actual event trees for this and other cases are discussed in great detail in Appendix I.

In summary, the event trees were the principal vehicles, supplemented by additional analyses, utilized for achieving a systematic determination of the radioactive release magnitudes and probabilities associated with potential nuclear power plant accidents. They first were utilized to identify the many possible significant accident sequences. Then, through an iterative process involving successive improvements in the definition of failure probabilities, the incorporation of system interactions and the resolution of physical process descriptions, they provided for the identification of those accident sequences that are important to the achievement of a realistic risk assessment. These selected accident sequences served as the basis for determining the magnitude of applicable radioactive releases (section 4.2.3). They also served as the vehicle for combining the initiating event probabilities, system failure probabilities, and containment failure probabilities into the composite probabilities applicable to the radioactive releases. With respect to system failure probabilities, the event trees were the principal means of identifying the various system failure definitions needed in the fault trees that were used for determining system failure probabilities.

4.2.2 PROBABILITY OF RELEASES

As noted previously, there were a large number of iterations in various parts of the risk assessment cycle described in this chapter. These iterations were necessary in order to determine the dominant accident sequences for use in the final overall risk assessment. The methods described below were utilized in this iterative process and aided in the selection of the dominant accident sequences. However, such iterations and other exploratory analyses are neglected in the following discussion, which is generally concerned with the determination of the radioactive release probabilities for the final overall risk assessment.

The final risk assessment is based on a number of different release categories. Each of these release categories is associated with a specific type and magnitude of release (see section 4.2.3 and Appendix V). The final risk assessment requires the probability applicable to each of these release categories. In general a specific release category applies to many accident sequences but, because of the wide range in probability of occurrence of these sequences, it is found that only a few sequences determine the probability of occurrence of a particular category. Thus, the determination of the release probability associated with each release category required the determination and summation of the probability of occurrence of each of the dominant accident sequences in the category.

The probability of occurrence of an accident sequence is composed of the

initiating event probability, the failure probabilities of systems included in the sequence, and the containment failure probability. The probabilities for LOCA initiating events such as pipe breaks, vessel ruptures, transients, etc., were determined by deriving appropriate failure rates from available failure rate data. The large majority of the system failure probabilities were determined with the aid of the fault tree technique. This technique, discussed in the next section, is suited for analysis of failures of complex systems. To account for probable dependencies in failures of components and systems involved in the fault trees and event tree accident sequences, many special analyses were performed for the purpose of determining significant common mode failures. These analyses are discussed in section 4.2.2.3. The applicable containment failure modes are largely determined by the accident sequences and the various physical processes that can result from the accident sequences. The basis for the likelihood of containment failure modes was determined by fault trees and by the analysis performed in Appendix VIII, which analyzed the applicable physical processes.

4.2.2.1 Fault Trees.

As noted in section 4.2.1 the event trees define certain system failures whose probabilities are needed to determine the risk. In this study the fault tree method has been used to estimate the majority of these failure probabilities. The method uses a logic that is essentially the reverse of that used in event trees. Given a particular failure, the fault tree method is used to identify the various combinations and sequences of other failures that lead to the given failure. The technique is particularly suited to the analysis of the failure of complex systems. The effective utilization of this logic requires that the analyst have a thorough understanding of the system components and their functions. This section gives a general discussion of the fault tree method. A more detailed discussion is provided in Appendix II and Addendum I to this report.

The fault tree method is illustrated in Fig. 4-5 which shows the first few steps of a fault tree concerning loss of electric power to all engineered safety features (ESFs). In this case it is known that the electric power to ESFs would require both alternating current (AC) power and direct current (DC) power. The AC provides the energy needed but the DC is required by the control systems which turn on the AC. Thus, failure of each of these systems appears in the first level and they are coupled to the top event by an OR gate. This symbol signifies that either one failure or the other (or both) can cause the top event and that the probability of the top event is, to a close approximation, the sum of the probabilities of the two events in the first level. Thus, if $P_{AC} = 0.001$ and $P_{DC} = 0.001$, then $P_{EP} = 0.002$. The EP failure probability can be computed in this way if there are sufficient failure data to determine P_{AC} and P_{DC} directly. However, in general, such failures have not occurred often enough to provide meaningful statistical data and therefore, the analysis must proceed to lower failure levels. The next level is developed only for loss of AC power. In this case it is known that either offsite power (the electrical grid) or onsite power (the station diesel generators) can supply the needed energy. Failures of these systems are therefore coupled by an AND gate, indicating that both would have to fail in order to produce the failure above.

The above basic method is used to develop the trees until they have identified failures for which statistical data exist to determine their probability. In developing the tree, consideration is given to intrinsic component failures, human factors and test and maintenance. Detailed discussions of this point are provided in Appendices II and III. The probabilities of the failures are then assigned to the appropriate elements of the tree and the probability of the top event is calculated. For complex trees, such as those involved in this study, the aid of a computer program is utilized for computing the top event probability. In general the individual probabilities are obtained from a limited amount of experience data so they have an appreciable uncertainty associated with them. A computer code used in the study propagated these uncertainties using a standard statistical procedure and determined an uncertainty for the system failure probability.

Fault trees were developed for almost all the major individual systems represented in the event trees. These systems include the various ESFs and some of the normally operating plant systems. In some cases several different versions of a given system fault

tree were required, depending upon the accident conditions prevailing at the time the system failure is postulated. For example, the probability of failure of the ECCS may be different depending upon whether the containment spray system operates or fails. Such differences have been accounted for in the study.

There are a number of limitations in applying fault trees to a risk assessment of nuclear power plant accidents. The most important drawback is probably that detailed fault trees for complex systems are very time consuming to develop. Furthermore, there are different ways in which the logic can be developed. Thus two different analysts are likely to produce different trees for the same system. Although both trees may be logically correct and produce the same system failure probability, the fact that they appear to be considerably different can be misleading.

As with event trees, serious errors can be made if it is assumed that all failures are independent. A substantial amount of the effort in this study has been expended on the search for common mode failures. The fault trees and event trees have been extremely useful in helping define those common mode failures that can contribute to the overall risk.

As with event trees, there is no way of proving that a complex fault tree includes all the significant paths to failure. Generally, at some point in the analysis, the analyst must truncate his fault tree by assuming certain events are not significant. Thus, the accuracy of the tree depends appreciably upon the skill and experience of the analyst. Any modeling, of course, depends upon the skill of the analyst, however it is particularly important for fault trees where few explicit rules and guidelines exist. However, a good check on the logical adequacy and completeness of a fault tree is obtained when it is quantified and subjected to sensitivity studies. In general all the trees constructed in this study were found to go into more detail than was needed.

4.2.2.2 Failure Rate Data.

The study utilized failure rate data in two principal ways. They were used directly to establish the probabilities of major events (failures) for which fault trees were not constructed. Such uses included the determinations of the probabilities of initiating events such as pipe breaks and reactor vessel ruptures. However, the majority of failure data was utilized as input to the fault trees so that the probabilities of the system failures could be determined. This failure data included estimates of component failures, human errors, and testing and maintenance contributions.

The accuracy of the fault tree method is highest when component failure rates are based on data obtained from failures in systems identical to the one under analysis. In the case of reactors the experience of a few hundred reactor-years is not sufficient by itself to provide statistically meaningful probabilities for most of the required component failure rates. It has therefore been necessary to also use data from a much broader base of industrial experience.

In this study extensive searches have been made for sources of failure rate data. These are discussed in detail in Appendix III. Each source has been investigated to determine its appropriateness for application to nuclear plants. The conditions of service of most of the components in reactors are similar to conditions in many other applications, such as those in fossil-fueled plants and chemical processing plants. The compilations of such industrial experience are the basic source of most of the failure rate data used in the study.

Certain components of nuclear systems may be subjected to rather unique environments, particularly during serious accidents. Foremost among these environmental factors are radiation and high temperature steam. In the process of determining applicable failure rates, the study employed specialists in component reliability to assess the effect of such conditions on system components. Based on their assessments, component failure rates and their uncertainties were increased for the extreme environments.

The design specifications of the components of the ESFs require that they be qualified to operate under a variety of accident conditions. It is, of course, possible that certain components may fail to meet these special design conditions. To ascertain how likely such design errors may be, this study carefully reviewed the components in a selected number of important safety systems to determine how well the design specifications had, in fact, been satisfied. A detailed report of this effort is provided in Appendix X. Based on

these assessments, component failure rates were modified to account for the deficiences found.

A common criticism of the fault tree method is that the system failure probabilities are not meaningful because of uncertainties in the knowledge of applicable failure rates. In general, the failure rates used in this study have uncertainties of a factor of 10 or 100 (±3 or ±10). In a few cases the uncertainty is a factor of 1000 (±30). Based on these uncertainties, a Monte Carlo technique (see Appendix II) was used to calculate the uncertainty of the overall system failure probability. The study has used a log-normal distribution for all the uncertainties assigned to component failure rates. The log-normal distributions were combined in a statistical manner to account for the error contributions from different component failure rates.[1] It was found that even with the larger component failure rate uncertanties that were used, the system failure probabilities were sufficiently accurate to obtain meaningful values for risk evaluation.

4.2.2.3 Common Mode Failures.[2]

Common mode failures are multiple failures that result from a single event or failure. Thus, the probabilities associated with the multiple failures become, in reality, dependent probabilities. The single event can be any one of a number of possibilities; a common property, process, environment, or external event. The resulting multiple failures can likewise encompass a spectrum of possibilities including, for example, system failures caused by a common external event, multiple component failures caused by a common defective manufacturing process, and a sequence of failures caused by a common human operator.

Because common mode failures entail a wide spectrum of possibilities and enter into all areas of modeling and analysis, common mode failures cannot be isolated as separate study, but instead must be considered throughout all the modeling and quantification steps involved in the risk assessment. In the study, common mode and dependency considerations were incorporated in the following stages of analyses:

- Event Tree Construction
- Fault Tree Construction
- Fault Tree Quantification
- Event Tree Quantification
- Special Engineering Investigations

In the event tree development, common mode failures were first treated in the detailed modeling of system interactions. If failure of one system caused other systems to fail or be ineffective these dependencies were explicitly modeled in the event trees. The systems rendered failed or ineffective by the single system failure were treated in the subsequent analysis as having failed with probability of one and the analysis concerned itself only with the critical single system failure. The changes produced in event trees by these relationships often produced significant increases in predicted accident sequence probabilities since a product of system failure probabilities was replaced by a single system failure probability. The development of the containment event tree that relates various modes of containment failure to system operability states and the physical processes associated with core melt, as discussed in detail in Appendix I, also accounted for dependencies which were due to the initiating event.

The event trees also defined the conditions for which the individual fault trees were constructed. Particular system failures, i.e., the top events of the fault trees, were defined as occurring under specific accident conditions that frequently included the prior failure of other systems. The fault trees were thus coupled to other systems in the accident sequence, as well as to the particular, common, accident environments that existed. The fault trees were drawn to a level such that all relevant common hardware in the systems was identified. This depth of analysis permitted identification of single failures that cause multiple effects or dependencies. These included single failures that cause several systems to fail or be degraded, or cause redundancies to be negated. The failure causes modeled in the fault tree analysis include not only hardware

---

[1] Studies indicated that, with the wide ranges of uncertainties used herein for component failure rate data, the exact form of the distribution used had little effect on the results obtained.

[2] A more specific discussion of the treatment of common mode failure is contained in Addendum I to this report.

failures, but also include failures caused by human intervention, test and maintenance actions, and environmental effects. Thus, a spectrum of potential dependencies is incorporated in the fault trees. In many cases these additional causes, usually due to human or test and maintenance interfaces, have higher probability contributions to system failure than the hardware causes. In a number of cases these non-hardware actions result in failure probabilities (essentially single failure probabilities) that are high enough to dominate the system failure probability.

The fault tree quantification stage, in which system probabilities were numerically computed, incorporated dependency and common mode considerations throughout the calculations. The failure rate for a particular component included not only contributions from pure hardware failure (sometimes called the random failure rate), but also included applicable contributions from test or maintenance errors, human causes, and environmental causes. Human errors were investigated to identify causes of dependent failures if, for instance, the same operator could perform all the acts. Testing or maintenance activities were examined for causes of dependent failures, for example, when several components would be scheduled for simultaneous testing or maintenance. Components were examined for potential dependent failures that may arise as a result of the environments created by accidents. The quantification formulas treated both hardware and non-hardware contributions with their relevant dependencies. The quantification process included determinations of the maximum possible impacts from common mode failures which might exist but were not previously included in the analyses. These determinations indicated whether additional common mode failures could have significant impact on the computed accident probabilities. The applicable systems and/or components were reexamined to identify the ways, if any, in which such significant common mode failures could occur.

After the fault trees were quantified, the event tree quantification stage combined the individual fault tree probabilities to obtain accident sequence probabilities. Since a sequence in the event trees can be viewed in terms of fault tree logic, the same quantification techniques were used on the accident sequences as were used on the individual fault trees. Since multiple systems were analyzed, the couplings now included dependencies across systems.

As a final check on possible dependencies and common mode effects, special engineering investigations were performed to complement the modeling and mathematical techniques which had been used throughout the study. Those event tree accident sequences which dominate the probability of occurrence of the categories were carefully reexamined for any specific dependencies which may have been overlooked.

The probability versus consequence calculations involve several inputs which have no significant common mode failure contributions. The accident probabilities, the weather, and the population distributions used in the calculation of consequences are essentially independent of one another (see section 4.3).

4.2.3 MAGNITUDE OF RELEASES

This section discusses the manner in which the magnitude of the radioactivity release from the plant to the environment was determined. The release magnitude is influenced by three major factors; the amount and isotopic composition of radioactivity released from the core, the amount of radioactivity removed within the containment, and the containment failure mode. All of these are time dependent factors which influence the radioactive release magnitude. Thus, the accident sequences defined by the event trees were of particular value in establishing the release magnitudes applicable to each of the release categories noted previously.

As already noted, only those potential reactor accidents that lead to core melting affect the risk significantly. Thus, for the most part, the determination of the release of radioactivity from the reactor core involved the estimation of the fractions of significant radioactive isotopes that are released from cores melting under various conditions. The various conditions and timing of core melting were defined by appropriate analysis of the applicable accident sequences in event trees. A variety of experiments reported in the literature provides information on the radioactivity released from fuel under various conditions. Such information was used in the determination of the applicable release fractions. These determinations are described in detail in Appendix VII. This work resulted from the deliberations of a group of specialists, who have been conducting work in this area at National Laboratories. In general, the experiments on which these results

are based were carried out with relatively small samples of fuel. It is believed that, because of the large surface to volume ratio in such experiments compared to that which would exist in a molten core, the release fractions used in the study tend to overpredict the fraction released from a core. However, since no large scale experiments have been conducted, there is no experimental verification that reductions in the release fractions will in fact be observed. For this reason such potential effects were not taken into account in establishing the release fractions applicable to the various release categories.

Radioactivity released from the core is subjected to a variety of physical processes that reduce the amount of radioactivity available for release to the environment. These processes include wash out by the fission product removal systems, natural plate out and deposition processes on surfaces within the containment, radioactive decay, and the effects of filters. These processes, coupled with the fuel release and the mode and timing of containment failure, are the major determinants of the magnitude of radioactive release to the environment. To account for all these effects a computer code called CORRAL was developed. It is described in detail in Appendices V and VII. The various parameters used in the code are based on recent investigations, conducted at National Laboratories, of the transport of radioactive materials within containments. The CORRAL code output is the quantity of each of 54 biologically significant isotopes released to the environment as a result of a given accident sequence, as indicated in Appendix VI.

Many of the accident sequences involve similarity in core melting, similarity in radioactivity removal processes, and the same containment failure mode. This permitted classification of accident sequences into a number of different types called release categories. Thus, the releases produced by core melt are characterized by several different categories, each involving a particular composition, timing and release point.

The work outlined above provided the information for composite histograms of the type shown in Fig. 4-2, that represent the probability and magnitude of the radioactive releases associated with each consequence category. The specific results for each type of reactor are reviewed in Chapter 5 and are discussed in detail in Appendix V.

4.3 CONSEQUENCES OF RADIOACTIVE RELEASES

The objective of this task was the prediction of the public consequences that result from the radioactive releases defined by Task I (section 4.2). The consequence predictions serve as the primary input to Task III (section 4.4), the overall risk assessment. The consequences of a given radioactive release depend upon how the radioactivity is dispersed in the environment, upon the number of people and amount of property exposed, and upon the effects of radiation exposure on people and contamination of property. These major elements of the consequence predictions are indicated in Fig. 4-6, which shows the principal subtasks involved in this task (Task II).

The dispersion of the radioactivity is determined principally by the weather conditions at the time of release and the release conditions, i.e., ground level, elevated, hot, cold, extended or puff. The population distribution as a function of distance is known for each of 68 reactor sites either in use or planned. The probable effects of radiation on people and property are based on available information on such effects. The calculational model developed in this study is described in Appendix VI.

The probability associated with a specific consequence is determined by combining the probabilities of the individual input parameters, i.e., by multiplying $P_{release} \times P_{weather} \times P_{population}$. In determining the consequence probability in this way, it is necessary to assure the probabilities are reasonably independent. It is difficult to visualize that the accident and the population densities can significantly affect one another. It seems equally reasonable to assume that the population and the weather have no strong dependency, since the frequency distributions have been obtained by combining actual meteorological and demographic data applicable to a large number of sites. It could also be argued that violent weather might cause an accident. Although this is highly unlikely because of reactor design requirements, it is not impossible. However, violent weather is characterized by extremely high turbulence which would cause very rapid dilution of the radioactivity and this would drastically reduce the consequences. The reduced consequences would likely counteract any probability increase associated with such a dependency, resulting in a negligible effect on the overall risk. Thus, it is reasonable to assume that

the three probabilities are independent and a straightforward multiplication is justified.

4.3.1 ATMOSPHERIC DISPERSION MODEL

The computer code uses the standard Gaussian Plume Model (Ref. 2), with the modifications noted below, to predict the way radioactivity is dispersed in the atmosphere. The release conditions are defined by the accident sequences. Each one of the release categories identifies the amount of radioactivity released, the amount of heat released with the radioactivity, and the elevation of the release (see Table 5-1 in section 5.2.1). A much more difficult problem is presented by the weather which can change in a large variety of ways during the dispersion of radioactivity. No completely realistic method now exists for treating dispersion of pollutants and existing models are felt to be particularly uncertain at long distances from the point of release.

The Gaussian plume model characterizes weather in six stability classes, A through F. Weather type A is unstable and type F is very stable. Wind speed is also required as an input to this model. The rate of dispersion for various types and wind speeds is characterized by parameters that give the spreading rate in the horizontal and vertical directions. In the study's model, the effects of rain are accounted for by adding a rate for washout of radioactivity from the plume during the period when rain occurs. In all cases the radioactive plume is contained below a mixing height characteristic of the site, season and time of day. A number of conservatisms exist in the model in that it does not account for the effects of wind shear, changes in wind direction, ground decontamination factors due to rain, or the potential for strongly heated releases to penetrate the inversion layer.

The weather data used in the model is obtained from hour by hour meteorological records covering a one year period at six sites that would typify the locations of the first 100 large nuclear power plants. Ninety weather samples are taken and each sample is thus assigned a probability of 1/90. The starting times are determined by systematic selection from the various sets of applicable meteorological data. One quarter of the data points are chosen from each season of the year and half from each group are taken in the daytime. This procedure is used to reduce sampling errors to acceptable levels. The weather stability and wind velocity following the accident is then assumed to change according to the weather recordings made at the site. The weather model calculates, for each of 54 radioisotopes important to the prediction of health effects, the concentrations of radioactivity in the air and on the ground as a function of time after the release and distance from the reactor. Further details of the weather model are presented in Appendix VI.

4.3.2 POPULATION MODEL

To determine the population that could be exposed to potential releases of radioactivity, census bureau data is used to determine the number of people as a function of distance from the reactor in each of sixteen 22 1/2° degree sectors around each of the sites at which the 100 reactors covered by the study are located. Each reactor has been assigned to one of the six typical meteorological data sets and a 16 sector composite population has been developed for each set.[1] Three of these sectors are those which have the largest cumulative population (within 50 miles of the reactor) of all the sectors associated with reactors assigned to that set. The probability of exposing people in these sectors is

$$P_{\substack{\text{exposure} \\ 1,2,3}} = \frac{1}{16 \times N}$$

where N is the number of reactors assigned to the set. The other 13 sectors of a typical set are obtained in the same way, except that groups of sectors with approximately the same population density are combined to obtain the population as a function of distance. These sectors were given a probability of exposure of:

$$P_{\substack{\text{exposure} \\ 4 - 16}} = \frac{n}{16 \times N}$$

where n is the number of sectors combined. In this combination process,

---

[1] The data used was selected to be typical of eastern valleys, east coast, southern, midwestern, lakeside, and west coast sites.

the n radial sectors are averaged at each mesh point distance to give the value used.

In the case of a potentially serious accidental release, it is assumed that people living within about 25 miles of the plant, and located in the direction of the wind, would be evacuated in order to reduce their exposure to radioactivity. An evacuation model to represent this process has been developed and is described in Appendix VI. This model is based on the study's analysis of data collected on a substantial number of actual evacuations that have taken place in the United States (Ref. 3).

4.3.3 HEALTH EFFECTS AND PROPERTY DAMAGE MODEL

The consequence model calculates the doses from five potential exposure modes; the external dose from the passing cloud, the dose from internally deposited radionuclides which are inhaled from the passing cloud, the external dose from the radioactive material which is deposited on the ground, and the doses from internally deposited radionuclides which are either inhaled after resuspension or ingested from ground contamination. The models used for calculating these doses are described in Appendix VI.

The potential health effects calculated are early fatalities (i.e., fatalities that occur within one year of the accident), early illnesses (i.e., people needing medical treatment), and late health effects that are estimated from the total man-rem dose to the population. Late health effects may include lethalities from cancers, thyroid illnesses, and genetic effects that can potentially occur at long times after the time of the accident. Radiation exposure information does not provide clear distinctions between probable deaths, injuries and long term effects. As discussed in detail in Appendix VI, the probability of early fatalities and illnesses are computed by using a dose effect relationship. For whole body exposures, the probability of early fatality varies from 0.01 to 99.99% for doses of 320 and 750 rads respectively, with a median value of 510 rads. The principal early illness involves respiratory impairment whose probability of occurrence varies from 5 to 100% for doses to the lung in the range of 3000 to 6000 rads respectively. The incidence of latent cancer fatalities and genetic effects are based on the BEIR report with some modification of the former to account for dose rate and dose magnitude dependencies. In addition to whole body effects and doses to the lung, thyroid gland and GI tract doses are also calculated. The effect of thyroid doses is to increase the occurrence rate of thyroid nodules, a portion of which are expected to become cancerous. Since thyroid nodules can be treated very effectively, it is expected that few, if any, deaths will result from thyroid irradiation.

The consequence model also provides for prediction of property damage due to radioactive contamination. It also includes costs associated with relocating people for the time needed to decontaminate their property. Property damage costs are calculated on a per capita basis relative to the total value of property and land in the United States including appropriate values for the loss of agricultural crops. This aspect of the model is discussed further in Chapter 5 and in considerable detail in Appendix VI.

4.4 OVERALL RISK ASSESSMENT

The analysis of accident consequences described in the preceding section yielded the probability/magnitude relationships for each of the specific consequences - early fatalities, early illness, thyroid illness, latent cancer fatalities, genetic effects, property damage, and land contamination. Together, these seven distributions, which are provided and discussed in Chapter 5, represent the overall public risk from potential nuclear power plant accidents involving nuclear power plants of current design. For reasons discussed in section 2.4, no attempt has been made to consolidate the various consequence types into a single probability/magnitude distribution in which the various types of consequence are represented by a single common unit.

References

1. Raiffa, H., "Introductory Lectures on Making Choices Under Uncertainty", Addison-Wesley, 1968.

2. Slade, D. H., "Meteorology and Atomic Energy 1968," U.S.A.E.C., Division of Technical Information, TID-24190.

3. Hans, J. M. and Sell, T. C., "Evacuation Risks - An Evaluation" Office of Radiation Programs, National Environmental Research Center, Las Vegas, Environmental Protection Agency, EPA-520/6-74-002, June 1974.

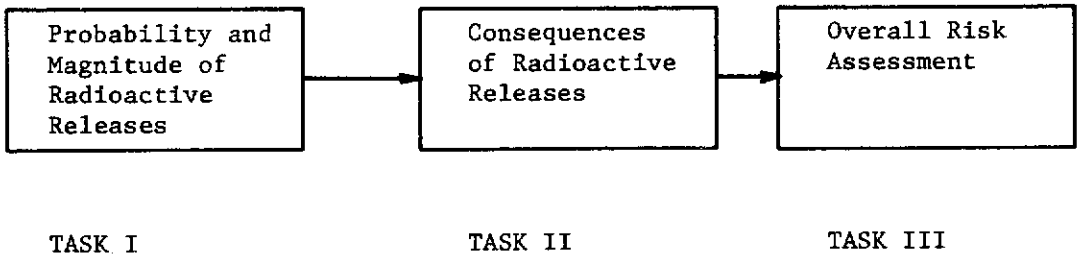


FIGURE 4-1 Major Tasks of Study

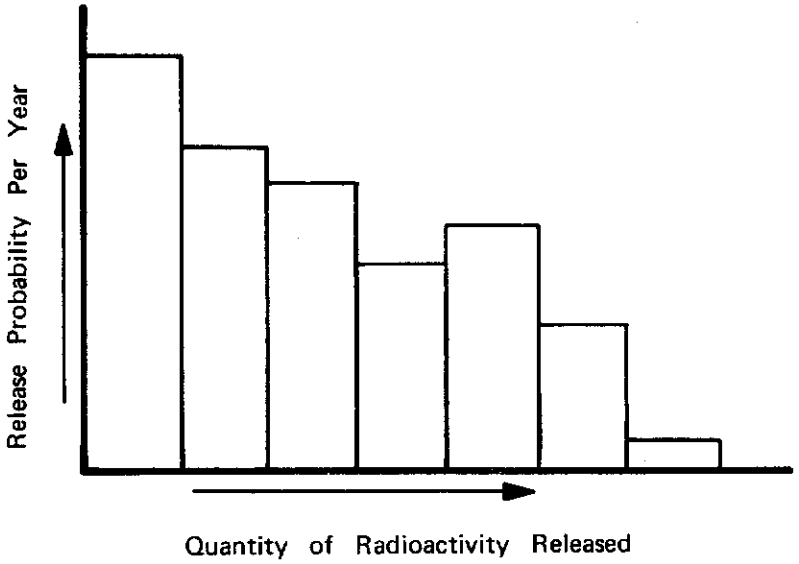


FIGURE 4-2 Illustrative Release Probability Versus Release Magnitude Histogram

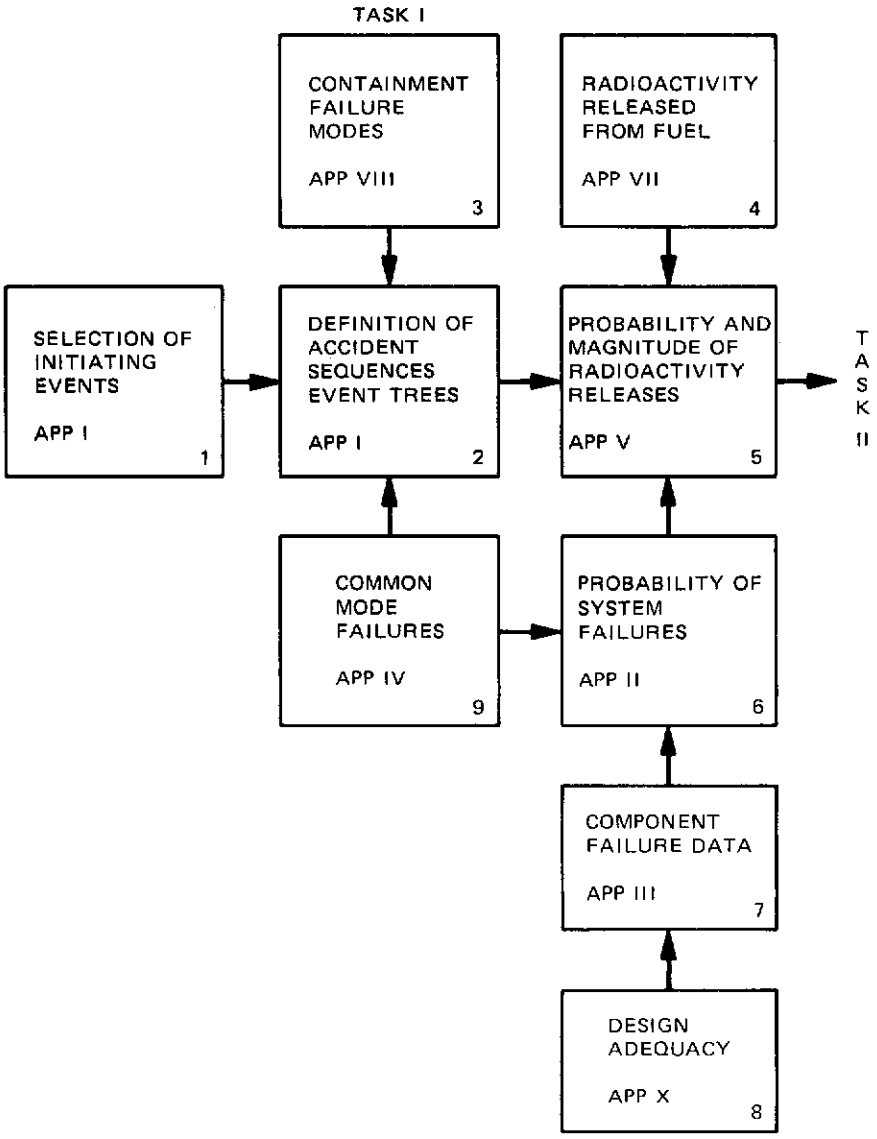
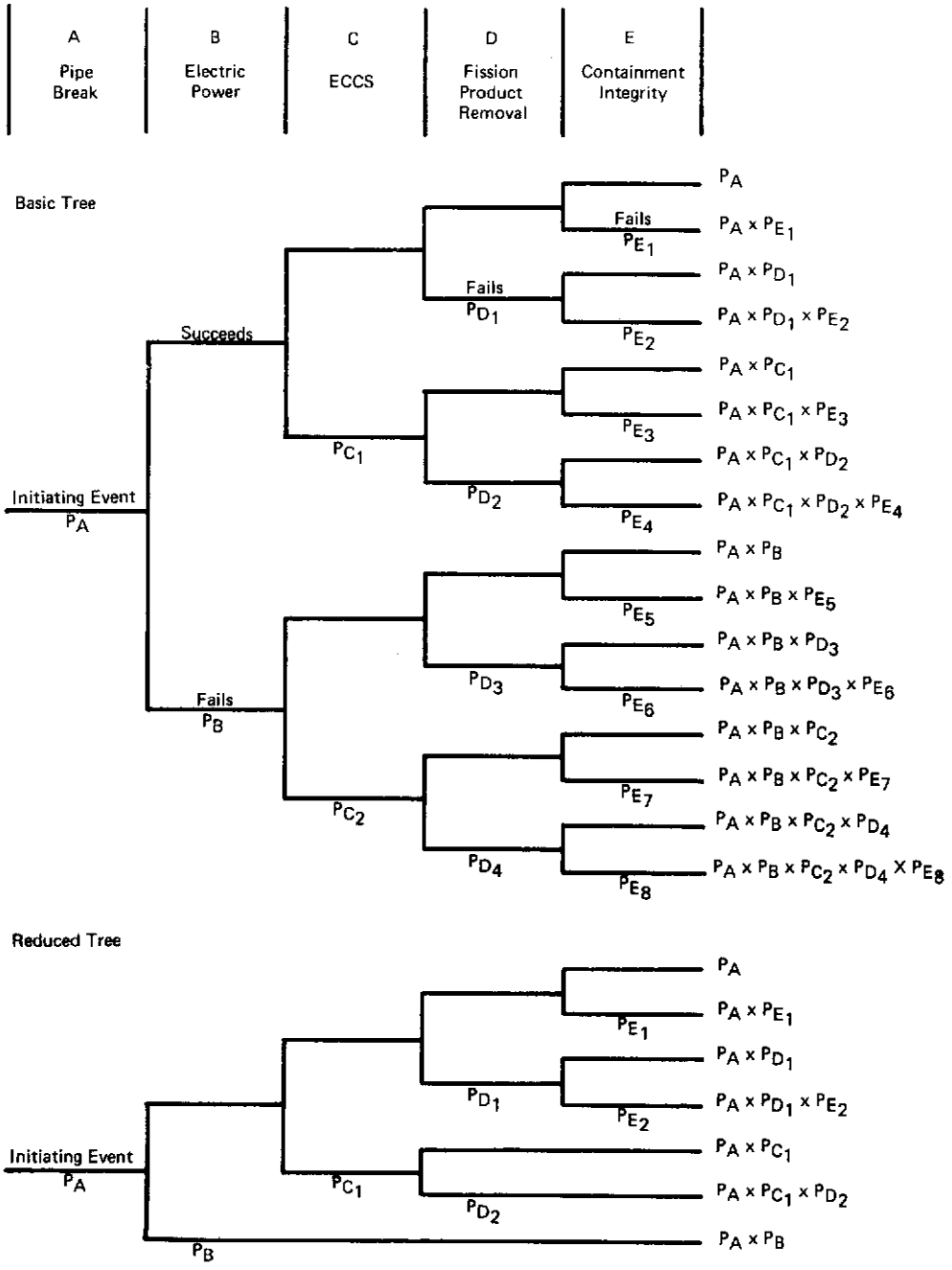


FIGURE 4-3 Subtasks in the Quantification of Radioactive Releases



Note - Since the probability of failure, P, is generally less than 0.1, the probability of success (1-P) is always close to 1. Thus, the probability associated with the upper (success) branches in the tree is assumed to be 1.

FIGURE 4-4 Simplified Event Trees for a Large LOCA

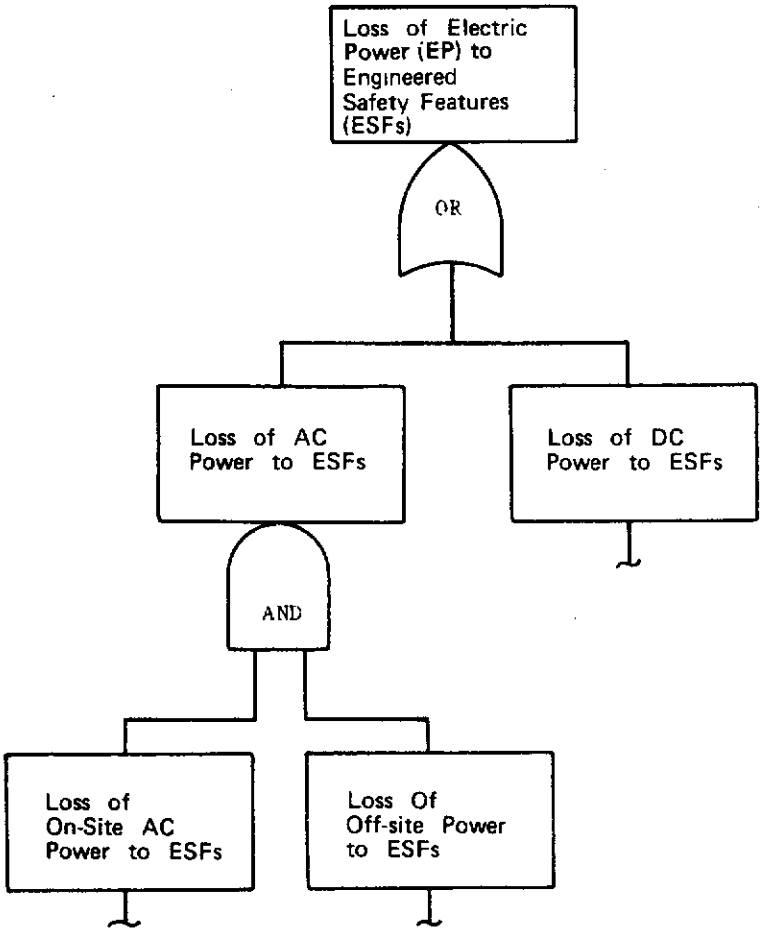


FIGURE 4-5 Illustration of Fault Tree Development

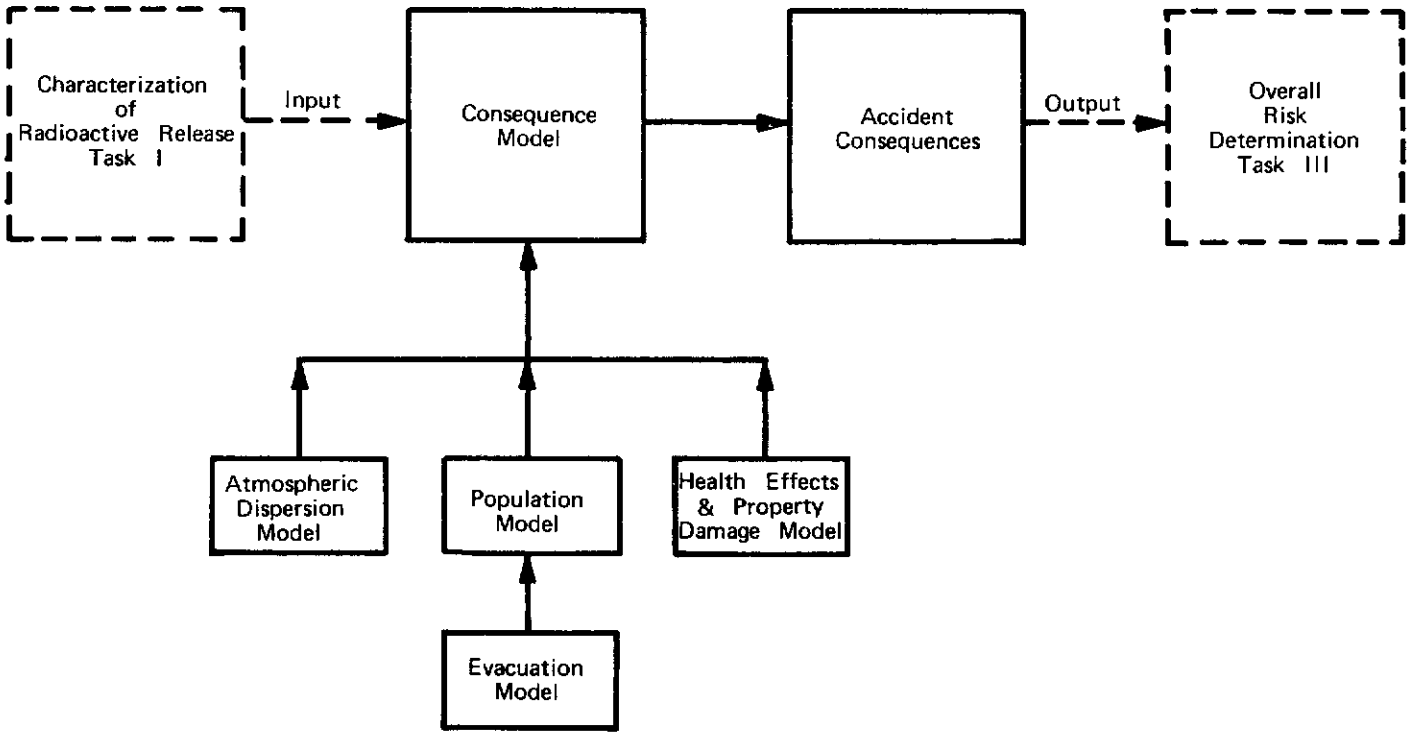


FIGURE 4-6 Subtasks in the Determination of the Consequences of Radioactive Releases Task II (Appendix VI)

Chapter 5

Reactor Accident Risks

5.1 INTRODUCTION AND SUMMARY

This chapter presents the results of the nuclear plant accident risk assessments. These assessments, made according to the methodology outlined in Chapter 4, are fully described in the appendices to this report. Although the information presented in this chapter derives, to some extent, from all appendices, the majority of the study results reported herein come from Appendix V - Quantitative Results of Accident Sequences and Appendix VI - Calculations of Reactor Accident Consequences.

Section 5.2 describes how the radioactive releases associated with nuclear plant accidents are categorized and notes the principal characteristics of the different release categories. Section 5.3 provides the probabilities associated with each of the release categories and describes the dominant accident sequences, i.e., those that contribute significantly to the probability associated with each release category. Section 5.4 discusses the initiation of nuclear plant accidents by external causes, noting that deliberate human acts are not accounted for in the risk assessment. While the initiation of core melt sequences by earthquakes, tornadoes, floods, aircraft impacts, and tidal waves is possible, the probabilities are expected to be low and their contribution to risk is predicted to be small compared to that of the dominant accident sequences discussed in section 5.3. A discussion of nuclear plant accident risks, in terms of fatalities, injuries, long-term health effects, and property damage is provided in section 5.5.

Sections 5.2 - 5.5 provide summaries of the information that serve as the basis for predictions of the accident risks associated with a total of 100 nuclear power plants in the U.S. These predictions are discussed in section 5.6.

5.2 RADIOACTIVE RELEASE CATEGORIES

As set forth in Chapter 4, the quantities of various isotopes released from the containment following a given accident are calculated using the CORRAL Code described in Appendices V and VII. Rather than calculate each of the approximately 1000 core melt sequences with CORRAL, it seemed desirable to reduce the number to be calculated to those necessary to adequately determine the accident risk. To achieve this objective, the core melt sequences involved in the large LOCA event tree were carefully reviewed to identify those involving distinctly different physical processes and different combinations of ESF system failures.

5.2.1 PWR RELEASE CATEGORIES

In reviewing the PWR accident sequences it was found that the large majority of the sequences in all the event trees involved quite similar processes. It was thus possible to group the sequences into the one of 38 cases involving differences in timing or physical processes taking place during the accident. Each of these 38 cases was then analyzed using the CORRAL Code to obtain the magnitude of radioactivity released to the atmosphere. From these results it was found that the spectrum of releases could be well represented by a set of nine different radioactive release categories. These categories are shown in Table 5-1. This table includes additional items of information which will be discussed later.

One of the largest releases, category 1, is associated with a potential steam explosion in the reactor vessel. Such accidents would involve a large volume of molten UO_2 falling into a pool of water in the bottom of the reactor vessel, and becoming finely dispersed in the water to mix efficiently enough with it to produce a steam explosion. This could potentially release large enough amounts of energy to rupture the vessel and, in some cases, even the containment as a result of missiles generated by the vessel rupture. Because of the heavy concrete shielding around the reactor vessel, a missile having sufficient energy to rupture the containment would almost certainly go up through the containment dome. The one half of the molten core that was finely dispersed in water is assumed to be ejected into the containment oxidizing atmosphere, thus producing a large release, energetically discharged, from the upper part of the containment. Although such a release is predicted to be very unlikely, it cannot be ruled out completely on the basis of

present evidence. This category also involves failure of the radioactivity removal systems that are located in the containment.

The category 2 releases are also associated with core melt and basically involve failure of radioactivity removal systems to operate, followed by rupture of the containment caused by hydrogen burning and steam over-pressure. Category 3 includes some of the cases that are similar to those in categories 1 and 2, but involve partial success of radioactivity removal systems. Category 4 involves core melt cases in which the containment is not fully isolated and the containment radioactivity removal systems have failed. Category 5 is similar to 4 except that radioactivity removal systems are operating. Categories 6 and 7 cover cases in which the molten core melts through the bottom on the containment, with and without radioactivity removal systems operating, but the above ground part of the containment remains intact. In categories 8 and 9 the core doesn't melt, and only some of the activity in the gaps of the fuel rods is released. Category 8 involves gap releases with failure of the containment to isolate properly. In category 9, the containment isolates correctly.

Considerable effort was spent in trying to identify possible accidents in which a release larger than that of category 1 might be produced. The possibility of processes that might physically eject the entire core outside the containment was examined. No such process could be identified that appeared to be consistent with the energy available and the physical constraints of the containment. Even if such an event were to occur and the core melted outside of containment, a release larger than that of category 1 would not be expected to occur. This is so because these accidents already involve a large energetic dispersal of the molten fuel in the form of small particles where the large surface to volume ratio enhances both fuel oxidation and the release of radioactivity from the fuel.

5.2.2 BWR RELEASE CATEGORIES

The paths to release of radioactivity in a BWR are quite different than for the PWR. Although the BWR has containment sprays, they are not designed as ESFs and are not credited for removal of radioactivity. Further, the vapor suppression system that has some capability for removal of radioactivity is largely ineffective in a number of the core melt cases. Thus the principal mechanism for removal of radioactivity is natural deposition on the surfaces inside the containment and the reactor building. For these reasons, the BWR release categories are different than those for the PWR.

As in the PWR, the release categories were determined from CORRAL Code runs of those accident sequences involving different physical processes. Twenty-three CORRAL runs were made, and subsequent analyses identified the five release categories shown in Table 5-1.

As in the PWR, category 1 involves a steam explosion in the reactor vessel in which about half the core is involved. The steam explosion ejects this half of the core from the containment. The resulting exposure of the finely dispersed molten fuel to an oxidizing atmosphere results in a very large release of radioactive material to the atmosphere.

Category 2 involves a core meltdown after containment overpressure rupture caused by loss of decay heat removal systems. In this category a limited amount of deposition of the radioactive materials occurs and the release is made directly to the atmosphere. The magnitude of release is roughly comparable to category 1 for a number of the isotopes.

Category 3 covers overpressure ruptures of containment similar to category 2 but in this category the radioactive materials released from the core escape through the reactor building to the atmosphere. The radioactive release magnitude is smaller than category 2 releases since deposition and some scrubbing action by the torus water enhances retention of the radioactivity.

Category 4 covers the cases in which the containment fails to properly isolate and the leakage is enough to prevent containment overpressure rupture. In this category, the magnitude of radioactivity release is significantly reduced by additional deposition in the containment due to the longer release times and by deposition in the reactor building. In some cases, processing through gas treatment systems achieves further reductions.

Category 5 covers the case where the core does not melt and a small amount of

activity may be released from the gap of the fuel rods. The small amount of radioactivity which may then leak from containment is further reduced by processing through the reactor building gas treatment system, which includes filtration. The release to the atmosphere then occurs through a tall stack.

5.3 PROBABILITY OF RELEASE

This section presents the probabilities associated with each of the radioactivity release categories for the PWR and BWR and the technique used to establish the probability values and to account for uncertainties in the magnitude of release for various categories is identified. In addition, those accident sequences that were found to dominate the probability of the respective PWR and BWR release categories are described.

5.3.1 PWR RELEASE PROBABILITY

All of the PWR event tree sequences were assigned to one of the release categories described in section 5.2. These assignments were made on the basis of their similarity to one of the 38 CORRAL Code runs. Those sequences which contributed significantly to the probability of each category are called dominant sequences and are listed, for each event tree, in Table 5-2, along with their probabilities and the explanation of the sequence symbols. The median values at the bottom of the table were used to generate the PWR histogram shown in Fig. 5-1, with the error bars representing the 90% confidence limits.

It should be noted that the probabilities for the individual sequences do not always add up to the median values at the bottom of the table. There are two reasons for this. First, as described in Appendix V the probability distribution of the final values are obtained by a Monte Carlo process which samples from the distribution of possible values in each of the quantities being combined. The result of this process may make the median value slightly larger than an arithmetic summation when significant uncertainties exist. The second reason for the differences is that 10% of the probability for each category is assigned to the next larger category and 10% to the next smaller. This process is described in section 4.1.2 Appendix V and was used to account for uncertainties in the magnitude of the releases involved in the sequences assigned to the various categories. Thus, although the sequences in category 6 have a probability of $<10^{-6}$, the value assigned is 6×10^{-6} to account for the 10% chance that some of the sequences in category 7 may produce a category 6 release.

The values in the histogram shown in Fig. 5-1 were used as an input to the consequence calculations of the PWR.

5.3.2 PWR DOMINANT ACCIDENT SEQUENCES

A detailed discussion of the dominant PWR accident sequences leading to core melt is given in Appendix V. Brief summaries of the dominant contributors from each of the event trees are presented below. In this section, and in section 5.3.4, the dominant accident sequences for the PWR and the BWR are discussed. The probability for each accident sequence is given, along with its error spread. As previously discussed in Chapter 4, in determining the probability of an accident sequence, common mode dependencies must be incorporated throughout each step of the calculations. A sequence consists of three elements; initiating event, particular ESF failures, and the containment failure mode. Dependencies within each of the elements, and among the elements must be considered to ensure that realistic probability estimates are obtained.

As indicated in Appendix II, the individual ESF failure probabilities contain the quantification of dependencies within ESF systems, including dependencies due to the initiating event. Appendix I describes the containment failure mode modeling, covering the dependencies between various initiating events and ESF failures to the various containment failures. Appendices V and VIII provide the quantification of these dependencies.

The subsequent discussions will describe the various dominant accident sequences. In general, where single ESF failures are involved, the sequence probability will be represented merely by the product of the various probabilities, since the appropriate dependencies will have already been considered. Where more than a single ESF failure is involved, the discussion will identify any significant dependencies found between the systems. Appendix V discusses the methods and mathematical treatments for quantifying dependencies between ESF systems.

The same considerations pertinent to potential dependencies were used in connection with BWR dominant sequences.

5.3.2.1 Large LOCA (A).

A large LOCA(Event A) is defined as a reactor coolant system (RCS) rupture having a size larger than the equivalent of about a 6" diameter hole. The median probability of such an event is assessed at 1×10^{-4} per reactor-year (see Appendix III). The dominant sequences that contribute to core melt are AD-ε and AH-ε.

The AD-ε sequence is large RCS rupture followed by failure of emergency core cooling injection (D). This failure leads to core melt and failure of containment caused by the molten core melting through the bottom (ε). The median probability for failure of emergency core cooling injection was estimated by fault tree analyses presented in Appendix II. Possible common dependencies between the event A and the operation of the low pressure injection system (LPIS) were further examined and a dependency was identified, given that a rupture occurred in the RCS cold leg piping. This particular dependency, as discussed in Appendices IV and V, stemmed from the possibility that a missile from the flywheel of the main coolant pumps could disable the LPIS. With this dependency considered, the median value of the probability for the combined sequence AD was predicted to be about 2×10^{-6} with approximately an order of magnitude error spread. The spread is dominated by the uncertainty of the probability of a large pipe break. Since the containment ESFs operated successfully in this sequence, the probability of containment failure occurring via a melt-through (ε) was estimated to approach unity.

The AH-ε sequence is a large RCS rupture followed by failure of the emergency core cooling recirculation system (H). This failure leads to a core melt followed by the ε mode of containment failure. The median probability value for failure of the emergency core cooling recirculation phase was determined to be about 6×10^{-3}. This value depended largely on human error since successful operation of the core cooling system depends on the plant operator to make proper alignments of the system following completion of the injection phase operation. As in AD-ε, the range of uncertainly of the AH-ε sequence is also dominated by the probability of a large pipe break, and the calculated median value of the probability of this sequence is 1×10^{-6} per year.

As indicated by Table 5-2, these sequences lead to category 7 releases which are quite small since the containment failure mode, ε, results in the molten core melting into the ground beneath the reactor where a large fraction of the radioactivity is trapped in the soil. The AD and AH sequences can also lead to other modes of containment failure that give higher releases at a lower probability. For example, the AH-α and AD-α sequences, involving steam explosions in the reactor vessel, appear in category 3, but at a probability that is a factor of 100 less the ε sequences.

The total probability of core melt resulting from the large RCS rupture initiating event is approximately 3×10^{-6} per year. The dominant contributors to this probability are sequences AD-ε and AH-ε. These occur in release category 7 and are significantly smaller than the total probability of 4×10^{-5} per year for that category. Examination of Table 5-2 also indicates that none of the other less probable large LOCA sequences makes any significant contribution to their release categories. Therefore, the large LOCA event tree is a minor contributor to the release histogram.

5.3.2.2 Small LOCA (S_1).

The small LOCA (S_1) is defined as an RCS rupture of between 2" and 6" equivalent diameter. It has a median probability of 3×10^{-4} per plant per year (see Appendix III). The dominant sequences are S_1D-ε and S_1H-ε as in the large LOCA. S_1D-ε has a probability of 3×10^{-6} and S_1H-ε a probability of 3×10^{-6}.

The total probability of core melt by S_1 type LOCA events is about 6×10^{-6} per year, with an error band of about 10. Again, this is mainly due to uncertainties in the probability of the initiating event.

Although the S_1 events are not the largest contributors to core melt they are only a factor of about 3 less likely than the more likely contributors and so their contribution to category 7 must be considered. As can be seen from Table 5-2, however, S_1 events are not significant contributors to other release categories. Because category 7 represents a small release, S_1 events will contribute very little to the overall consequences of core melt.

5.3.2.3 Small LOCA (S_2).

The small LOCA (S_2) is defined as an RCS rupture of between 1/2" and 2" in equivalent diameter. This event has a median probability of 10^{-3} per reactor-year, or 10 times larger than that for a large RCS rupture. The dominant sequences are S_2D-ε and S_2H-ε, as in the A and S_1 sequences discussed above. The probabilities of these two sequences are about 9×10^{-6} and 6×10^{-6}, respectively. Note that these probabilities are not exactly 10 times those for the corresponding sequences in a large LOCA event tree since, under S_2 LOCA conditions, the probability of failures D and H are somewhat smaller because different subsystems of the emergency core cooling system perform these functions.

The median probability of core melt caused by S_2 events is 2×10^{-5} per year, with an error band of about three that is principally due to uncertainties in the probability of the initiating event.

The S_2 sequences contribute the largest probability to PWR core melt. While the probability of a small LOCA is 10 times more likely than a large LOCA, the availability of the high pressure ECCS required to cope with these accidents is not significantly higher than that of the low pressure ECCS for large ruptures. The S_2 events dominate categories 3, 4, 5 and 6 in the PWR release histogram, although both S_1 and transient events (T) are important contributors to some of these categories.

5.3.2.4 Reactor Vessel Rupture (R).

The reactor vessel rupture event (R) is defined as a vessel rupture large enough to negate the effectiveness of the ECCS systems required to prevent core melt. The median value of the probability of such an event is 10^{-7} per vessel per year as indicated in Appendix V. As indicated by Table 5-2, the R event is a negligible contributor to the PWR release histogram. Gross vessel rupture would have to be at least about 100 times more likely than the value estimated in order to contribute to the PWR core melt probability and to large consequence accidents.

5.3.2.5 Interfacing Systems LOCA (V).

The interfacing systems LOCA (V) is caused by the failure of check valves that isolate the low pressure injection system from the reactor coolant system. This event requires the failure of two in-series check valves. If this were to occur during operation, the 2250 psi reactor coolant system pressure would be imposed on the low pressure injection system (LPIS) which is designed for only 600 psi. It is predicted that the LPIS will almost surely fail under these conditions, so the probability of LPIS failure is taken to be near unity.

The result of this set of events is to produce a LOCA of $\sim$6" effective diameter, which also fails the low pressure injection system. In addition, the break in the system will lead into a safeguards building outside the containment so there will be a direct path for radioactive release to the atmosphere, thus bypassing the radioactivity removal systems. There will, however, be plateout of the less volatile radioactivity in the long LPIS pipe run and on the surfaces of the safeguards building.

The probability of this event has been calculated to be 4×10^{-6} per year. This value is somewhat large because a failure of one of the check valves is not detectable. If one check valve were to fail in an open position it will remain undetected in this failed position, and if the second check valve were then to rupture, the accident would occur. This situation gives rise to a failure dependency between the check valves that would not exist in a different testing program. As shown in Appendix V a monthly, independent test of these valves to assure their seating integrity would lower the probability of their combined failure by a factor of about 20. Although this sequence is not dominant in a low release core melt path, it produces releases principally in category 2 (because of the containment failure) and thus dominates the probability of the high releases in the PWR release histogram.

5.3.2.6 PWR Transient Events (T).

As discussed in Chapter 3, transient events refer to a wide range of conditions that require the reactor to be shutdown. These include all unplanned shutdowns. Experience has shown that such events occur at the rate of $\sim$10 per year. Following the transient event, one of the shutdown systems must operate and, subsequent to that, operation of systems to remove core decay heat are required. Transient sequences involving failure to trip the reactor control rods are not important contributors to transient-produced core melt situations because of the relatively low failure probability (about 4×10^{-5}) of the shutdown systems and the additional pro-

tection against core melting provided by RCS safety valves and auxiliary feedwater. Thus, sequences involving failure to trip (K) do not appear as major contributors in any category of Table 5-2. The dominant transient contributors are the TML sequences. These are transients in which the decay heat removal systems fail, principally due to unavailability of both offsite and onsite AC power. The systems involved in TML include the normal power conversion system (M) and the auxiliary feedwater system (L).

Analysis of the event tree, as indicated in Appendix V, indicates that the most likely way for TML sequences to develop is for transients to occur as a result of failure of offsite power since this failure will also cause failure of the power conversion system (M). Experience data shows that the probability of such transients is about 0.2 per reactor-year. With offsite power failed, the failure of auxiliary feedwater is 1.5×10^{-4} per demand (with offsite power available, this probability is 4×10^{-5}).[1] If offsite power can be recovered within about 1 hour, the power conversion system can be used to remove decay heat. The probability of not recovering offsite power within this time is 2×10^{-1}, based on experience data. Thus, TML sequences which involve the loss of power has a probability of $(.2 \times 1.5 \times 10^{-4} \times .2) = 6 \times 10^{-6}$ per year. However the consequences associated with core melt from TML will depend on the functioning of the containment ESFs being restored with electric power prior to the containment failure. About half the time, the electrical power will be recovered between 1 and 3 hours which is soon enough to operate these ESFs successfully to mitigate the radioactivity released from the melting core to containment. Thus the probability of the loss of power transient occurring without ESFs (TMLB') is 3×10^{-6} per year.

If the containment ESFs do not operate, then there exists a relatively high probability of about 0.6 that the containment will rupture in an overpressure mode (δ) and this would lead to category 2 releases. A smaller probability of about 0.2 exists that containment failure occurs via the containment melt-through (ε) which would then lead to a smaller category 6 release. Thus the loss of power transient that occurs without containment ESFs leads to a category 2 release with a probability of about 2×10^{-6} per year and a category 6 release with a probability of about 6×10^{-7} per year. These TMLB' sequences were found to be important probability contributors over the release spectrum.

If power is recovered such that containment ESFs operate, then the TML sequence has a high probability of being a category 7 release. Considering all the TML sequence contributions, e.g., transients other than the loss of offsite power, the overall probability of TML-ε sequences leading to a category 7 release was about doubled to 6×10^{-6} per year. As can be seen from Table 5-2, the TML-ε sequence was about equal to small LOCA (S_2) sequences in its contribution to the core melt probability.

Thus the transient sequences give significant, although not dominant, contributions to the PWR release histogram.

5.3.3 BWR RELEASE PROBABILITY

As in the PWR, all BWR event tree sequences were assigned to a release category based on their similarity to a sequence analyzed by a CORRAL run. The dominant sequences and their probabilities are listed in Table 5-3. The dominant contributors from each event tree are listed separately for convenience.

5.3.4 BWR DOMINANT ACCIDENT SEQUENCES

5.3.4.1 LOCA Events.

Although the probabilities of the initiating events were the same as those of the PWR, the combined availability of the ECC systems is better; thus the

[1] The reduced availability of the auxiliary feedwater system (AFWS) following the loss of offsite power is due, in large part, to dependencies of the system's electric pumps on the onsite emergency diesel generators. The diesel generator arrangement in this particular PWR design employs a swing diesel generator which is shared between two units on the site. When the loss of offsite power occurs, the swing diesel serves only one of the two units on the site, leaving the other unit without power to part of the AFWS. This dependency caused by the swing diesel arrangements results in a reduced AFWS availability for one of the two units as shown through fault tree analyses presented in Appendix II. It is of interest to note that the use of such swing diesel arrangements is a practice now discouraged by AEC licensing authority at multiunit sites.

probability of LOCA-caused core melts is less than 10^{-6} for all release categories and is not a significant contributor to any category. A more detailed discussion of BWR LOCA events is given in Appendix V. It should be noted that although the probabilities of LOCA induced core melts are smaller than in the PWR, they result in larger radioactive releases if they occur. This happens because the BWR containment volume is considerably smaller, and when the core melts, the noncondensable gases generated by the zircalloy-water reaction and molten fuel interaction with the concrete will overpressurize and rupture the containment. Thus, the most likely path to containment failure is by overpressure, rather than by melt-through. This failure also negates the reactor building filter system. Thus, those relatively small releases as seen in category 6 and 7 in the PWR for the melt-through path are not likely to occur in the BWR.

5.3.4.2 Reactor Vessel Rupture (R).

As with the PWR, reactor vessel rupture is defined as a vessel failure large enough to negate successful operation of the ESFs required to prevent core melt. Again, the probabilities of such events are small and make no significant contribution to the release histogram in Fig. 5-2.

5.3.4.3 Transient Events (T).

Transient events dominate the releases in all categories of core melt accidents except category 4 where the overlap from the higher releases in category 3 dominates. These transient events include a wide variety of conditions that require shutdown of the reactor. They include unplanned shutdowns that can be expected to occur during the life of the plant. No matter what the cause of shutdown, decay heat removal systems are required to operate to prevent core melt. Since about ten shutdowns per year can be expected based on plant operating experience, the decay heat removal system will be required frequently. The probability of failure of the decay heat removal systems (W) was determined (see Appendix V) to be 1.6×10^{-6}. When combined with the ten transients that occur per reactor-year, this yields about 2×10^{-5} for the TW sequence.

With the TW sequences, the probability of failure of containment by overpressure was considered to be near unity. Given overpressure failure, the release path for radioactivity can be either through the containment drywell and the reactor building where some deposition of the radioactive materials occur (γ) or more directly to the atmosphere (γ').

Due to plant layout, the probability of a release path (γ) through the reactor building is higher at about 0.8 and the path more direct to the atmosphere (γ') is about 0.2. These lead to category 3 (TW-γ) and category 2 (TW-γ') releases respectively, at a probability of about 1×10^{-5} and 3×10^{-6} per year. As can be seen from Table 5-3 these TW sequence probabilities are either equal to or larger than all other sequences. In category 3, the transient-caused core melts resulting from failure to achieve rapid reactor shutdown (TC) have a probability about equal to the TW-γ seqence. For these TC sequences the probability was also found to be about 1×10^{-5} per year, where the probability of failure to shutdown the reactor is about 1.2×10^{-6} per year. The TC sequences also lead to overpressure failure of containment (γ and γ') and this occurs during the core melt at a probability near unity. However because some of the radioactivity is retained by scrubbing action of the vapor suppression pool during the core melt, the magnitude of radioactivity released to the atmosphere is, unlike the TW sequence, not as sensitive to the release path.

5.3.5 OTHER INTERNAL CAUSES

Qualitative considerations pertaining to the potential for large electrical fires led the study to the conclusions that (1) the start of a fire in or near important components and cable spreading areas was a relatively low probability event by comparison with some other types of events evaluated, (2) the use of fire prevention and fire fighting techniques would limit the extent of the fire and its damage, and (3) even if a large fire occurred it would be unlikely, because of design requirements for separation of equipment and cables, to cause damage that might lead to a large release of radioactivity.

Recently a large fire in electrical cabling occurred at the Browns Ferry Nuclear Plant and this specific event enabled a more quantitative check to be made on the validity of the study's qualitative judgment. A somewhat conservative quantitative assessment was made of the course of events that occurred to estimate how close this fire came to causing unacceptable core temperatures and a potential release of radioactivity. The results of this as-

sessment indicated that the probability of a potential fire-induced core melt would be about 20% of that obtained from all other causes analyzed. Since this estimate of about 1×10^{-5} per reactor-year was found to be either covered by or fell within the band of uncertainty of other predictions made in this study, it seems reasonable to believe that, if the Browns Ferry fire is typical of the gamut of large electrical fires at nuclear plants, then the study's qualitative judgment about fires remains valid. It should be recognized however, that the quantitative assessment of the Browns Ferry fire necessarily concerned itself with the specific fire damage and events that occurred plus some potential variations from these specific events. Thus, the above conclusion may be of somewhat limited applicability.

One of the lessons that emerges quite clearly from the analysis performed is that there are rather straightforward measures, such as may already exist at other nuclear plants, which can improve fire prevention and fire fighting capability and that these can significantly reduce the likelihood of a core melt accident being caused by fires. The study also believes that it would be useful to further pursue the collection and analysis of data associated with fires as well as the development of a risk model for treatment of the effect of fires.

5.4 PROBABILITY OF RELEASES FROM EXTERNAL CAUSES

The probabilities and releases given in the previous section are associated with a variety of intrinsic failures that can potentially occur within a nuclear power plant. The data on which the probabilities are based include a wide variety of causes such as design errors, failures in QA and QC procedures, operating errors, etc. However they do not explicitly include consideration of potential failures due to large external events which might affect the plant. Events such as major earthquakes, floods, windstorms, aircraft impacts, etc., if they were to cause an accident, would have to produce core melt by one of the paths described by the event trees. The question is whether they could make the sequence probabilities estimated in the analysis in section 5.2 higher than they would be due only to intrinsic failures. It is important therefore to estimate the probabilities associated with these external events and determine if they are large enough to contribute significantly to the probability of the various release categories.

5.4.1 EARTHQUAKE RISK

Although it is difficult to predict with precision the probability of potential accidents due to earthquake damage to a nuclear power plant because of the general sparsity of quantitative data on the sizes and effects of earthquakes, it appears possible to make order of magnitude estimates that are useful in the type of risk assessment performed in this study. Recently published papers are of particular interest in this regard. These papers provide additional information on the approximate probability distribution of peak seismic accelerations in the U.S. (Ref. 1) and the probability of predicted seismic damage to safety systems installed in nuclear power plants (Ref. 2).

Hsieh et al. calculate the probabilities of ground accelerations of various magnitudes for both the Eastern and Western U.S. The analysis uses several of the currently published curves for earthquake probabilities and information on the attenuation of ground motion. It also uses the work of Brazee (Ref. 3) to obtain factors for the attenuation of earthquake forces with the distance from the earthquake epicenter. Typically, Brazee's results give areas above a specified Modified Mercalli Intensity (MMI) about four times larger than those used by Cornell (Ref. 4).

Since the probability of a point experiencing a given intensity is roughly proportional to this area, the probabilities that are predicted on the basis of Brazee's data will be about four times higher. Hsieh's work, as indicated in Table 6 which is reproduced below, gives the probability of occurrence of earthquakes as a function of acceleration at any given point in the Eastern U.S.[1]

---

[1] Eastern U.S. is meant to mean east of the Rocky mountains. The same type of analysis would apply to reactors located on the west coast. Although the frequency of earthquakes there is higher, reactors are designed to withstand higher SSE values so the overall probabilities predicted herein would not be significantly affected.

Table 6. Probability of Ground Acceleration per Year in the Eastern U.S. for Different Site Conditions

Ground Accel. (incremental)*	Soft	Average	Firm
0.1g	7.7×10^{-3}	3.6×10^{-3}	1.4×10^{-3}
0.2g	1.9×10^{-3}	6.5×10^{-4}	1.5×10^{-4}
0.5g	2.0×10^{-4}	4.6×10^{-5}	7.9×10^{-6}
1.0g**	3.5×10^{-5}	1.0×10^{-5}	6.9×10^{-7}

*The increment includes a band of accelerations around that specified, e.g., the probability at 0.1g is equal to the average of the two probabilities 0.5g to 0.1g and 0.1g to 0.15g.

**This entry encompasses accelerations greater than 1.0g.

TABLE B

Probability of Producing Failure of Two Systems, Given an Earthquake for Reactors Designed for an SSE of 0.2g.

Ground Acceleration	Newmark Factor	Prob. of Damage Single System	Prob. of Damage Two Systems	Error Factor
0.2g	20	.001	3×10^{-5}	30
0.5g	8	.02	3×10^{-3}	7
1.0g	4	.1	3×10^{-2}	3

The values in Table B can now be combined with the values of Table A to produce the values in Table C.

TABLE C

Probability of Producing Core Melt in Reactors Designed for SSE of 0.2g

Ground Acceleration	Probability of Ground Acceleration Average	Probability of Ground Acceleration Firm	Probability of Damage Two Systems	Probability of Core Melt (per reactor - year)[1] Average	Firm
0.2g	7×10^{-4}	2×10^{-4}	3×10^{-5}	2×10^{-8}	6×10^{-9}
0.5g	5×10^{-5}	8×10^{-6}	3×10^{-3}	2×10^{-7}	3×10^{-8}
1.0g	1×10^{-5}	7×10^{-7}	3×10^{-2}	3×10^{-7}	2×10^{-8}
			TOTAL	5×10^{-7}	6×10^{-8}

[1] If probability of damage to a single system is usual, which is equivalent to assuming complete dependence, then the 0.2g probability is increased by a factor of 30, the 0.5g probability by a factor of 7, and the 1.0g probability by a factor of 3. The total probabilities would then be approximately 3×10^{-7} for the firm case.

Although most U.S. reactors are located on firm sites, a few might be better termed average sites in the notation of Table 6. In this analysis, the results are computed on the basis of two assumptions:

a. All reactors are located on firm sites.

b. All reactors are located on average sites.

In order to estimate the probability of an earthquake producing a core melt accident, the probability of the earthquake (P_E) must be combined with the probability that the earthquake will produce enough damage (P_D) to cause potential accidents involving core melt (P_{CM}). Thus,

$$P_{CM} = P_E \times P_D$$

Newmark's work provides a basis for estimating the value of P_D. Figure 9 of his paper gives the probability of damage to safety systems in terms of the size of potential earthquakes. This figure indicates that the safety factor for reactor systems is about 20 for the SSE, and gives a system damage probability $P_D \simeq .001$ for that size event.

The analysis of potential core melt accidents indicates that generally two systems would have to fail to produce such an event. If the failure probability of any system is .001 then the probability that two would fail could be as low as 10^{-6}. However, it is reasonable to expect that, in some cases, the use of independent failure probabilities that would be implicit in a value of 10^{-6} may not be true. The potential for common mode failures between these systems should tend in general to increase the likelihood of their failure. On the other hand, if the systems were to have totally dependent failure probabilities, then their value would be 10^{-3}. Since neither of these extremes is likely, in the absence of more precise information a reasonable value for their joint failure would be the log normal mean, or 3×10^{-5} ± a factor of 30. The values in Table B were generated using this procedure and Newmark's data.

Thus if average sites are assumed, a value of 5×10^{-7} per reactor year is obtained; for firm sites the result is 6×10^{-8}. Since reactors are located principally on firm sites, a reasonable estimate is 10^{-7} and considering the uncertainties in damage probabilities, it seems reasonable to believe that the true value lies between 10^{-6} to 10^{-8}. At this level of probability, earthquake-induced accidents should not contribute significantly to reactor accident risks.

5.4.2 TORNADOES

All U.S. power reactors are now being designed to withstand the effects of sizeable tornadoes. The design basis tornado for the bulk of the country is assumed to have internal winds of about 300 MPH and to move with a translational velocity of about 60 MPH. It is assumed to develop pressure differentials of about 3 psi in 3 sec. In addition to withstanding the wind and pressure loadings, all vital reactor systems must be protected against tornado generated missiles. A review of tornado risks to reactors by Doan (Ref. 5) has recently been published. The main points are reviewed here.

The probability per year that a tornado will hit a given point can be expressed as:

$$P = \frac{an}{s}$$

where "a", the area affected, averages 2.8 square miles and "n" is the average annual frequency in an area of "s" square miles having tornado characteristics similar to the site where the reactor is located. Doan reports tornado strike probabilities of 10^{-3} - 10^{-4} per year for a number of reactor sites. The average for the reactor sites is about 5×10^{-4} per year. These estimates are comparable to those published recently by AEC's regulatory staff (Ref. 6).

The values above are the strike probability of a tornado of any size. A limited number of tornadoes have been carefully analyzed and internal wind velocities of 170 to 270 miles per hour have been estimated. Doan concludes that significantly less than 1% of all tornadoes would be expected to be as large as the design basis tornado. The probability of such a tornado striking a nuclear power plant would be on the average less than 5×10^{-6} per year.

The only seismic category I structures and equipment considered vulnerable to tornado damage are those associated with the emergency diesel-generators in each plant. The structural integrity and missile resistance of the diesel-genera-

tor buildings was examined as well as the vulnerability of the buried fuel storage tanks to penetration by planks and telephone poles. Except for the potential loss of the PWR diesel generator building doors following impact by the most energetic missile (leading to potential exposure of the associated diesel to the effects of wind-driven rain and hail), the diesel-generator buildings and fuel tanks were considered to be tornado-proof. Therefore, the probability of a tornado-caused core melt sequence is considered to be very small compared to the other core melt sequences.

5.4.3 FLOODS

All reactors on rivers subject to flooding must be designed to survive a hypothetical flood called the Probable Maximum Flood (PMF). This approach has been developed for the design of dams and other major structures subject to flood hazards. The PMF is based on an estimate made by combining the worst recognized values of all factors that contribute to producing a flood, rather than being based only on studies of observed flood frequencies. For example, the PMF on the upper reaches of the Mississippi River used in the analysis of the Monticello Reactor Site was developed as follows:

The heaviest snow pack observed in the last 100 years was subjected to the maximum temperature sequence. The resulting runoff was further increased by assuming that the largest postulated rainstorm occurred simultaneously over the entire area. The resulting river flow was 365,000 cfs and is nearly 10 times higher than the maximum observed flood of 47,000 cfs. In addition to the foregoing, the evaluation of reactor sites also includes, where appropriate, the potential effects of the failure of dams located upstream of the reactor site. These factors suggest that the approach to dealing with the effects of potential floods on reactors is generally quite conservative.

5.4.4 AIRCRAFT IMPACTS

The AEC has evaluated the probability of potentially damaging aircraft impacts at some sites located within five miles of airports. The probability for a potentially damaging crash per year at these sites was between 10^{-6} and 10^{-7} based on a conservative calculation. The majority of reactors are located farther than five miles from airports and will have significantly smaller probabilities of crashes than these sites. The probability for most plants would fall in the range of 10^{-6} to 10^{-8}. Because the containment is a fairly strong structure and the vital parts of the plant present quite a small area, these impacts would have a small probability of producing a core melt sequence. It is therefore concluded that aircraft impacts have a very much smaller probability of causing a core melt than the accident sequences already considered.

5.4.5 TURBINE MISSILES

The likelihood that the impact of a turbine missile could cause radioactivity to be released from the core or from the spent fuel storage pool indicate that events such as these are not expected to contribute to the overall risks.

Bush (Ref. 7) has estimated the probability of a turbine failure resulting in the generation of large missiles to be approximately 10^{-4} per year. He has also assessed the probability of missiles striking specific plant locations where systems could be affected and sources of radioactivity could be potentially released. For a typical PWR and BWR plant, the strike probabilities depend largely on the orientation of the turbine with respect to the strike area of interest and to the target area presented to the missile once it is generated by the turbine failure. The probability of damage being caused once the missile strikes a particular point depends largely on whether or not the missile is required to penetrate a substantial barrier, such as reinforced concrete structures, prior to damaging any particular component or system of interest. If, for example, the turbine missile is required to penetrate concrete barriers of thicknesses approaching 6 feet, then the probability of penetration approaches zero. On the other hand, the probability of penetration could approach one should a direct strike occur on concrete barriers having thicknesses of about three feet or less. Of course, the missile damage potential following such penetration would be reduced since much of its energy would be dissipated in the process. Review of the specific plant layouts for the PWR and the BWR plants used in this study indicated that the missile strike probabilities presented by Bush should provide a reasonably conservative representation of the strike probabilities to be expected. These are presented as follows:

Plant Structures	Limiting Missile Strike Probabilities
PWR	
Containment Wall	~0.24
Containment Dome	~8×10^{-3}
Spent Fuel Storage	~4×10^{-3}
Primary Auxiliary Bldg.	~1.2×10^{-3}
Diesel Generator Bldg.	~4×10^{-4}
BWR[1]	
Spent Fuel Storage	~6.7×10^{-5}
Rad Waste Bldg.	~4.8×10^{-3}
Control Room	~8.2×10^{-3}
Reactor Heat Removal Heat Exchangers	~3×10^{-4}
Diesel Generators	~6.4×10^{-3}

The highest strike probability for a turbine missile exists for the PWR containment wall principally because it presents a large target area. The containment wall thickness of about 4.5 ft. of reinforced concrete can possibly prevent the penetration of all but very energetic missiles. Assuming a probability of penetration of about 0.5, the overall probability for a turbine missile entering inside containment is approximately:

$$(A) \times (B) \times (C) = (D)$$

$$(10^{-4}) \times (0.24) \times (0.5) = 1.2 \times 10^{-5}$$

A = (Probability of Missile Generation by Turbine Failure (10^{-4}))

B = (Probability of Missile Strike (0.24))

C = (Probability of Missile Penetration of Structure (0.5))

D = (Probability of Missile Entering Structures (1.2×10^{-5}))

If the missile passes through the containment wall it will likely be stopped by the reinforced concrete crane wall which provides at least an additional two feet of thickness through which the missile would be required to pass before it reaches the operating floor above the reactor coolant system. The probability of the turbine missile causing damage to the reactor coolant system and a possible LOCA is thus negligibly small. Even if the missile does not penetrate the crane wall, it is possible that damage may be done to components located in the annulus between the containment and crane walls. The principal components located in this area of the PWR containment are the main steam pipes and it is possible that the missile along with spalled concrete could fall onto the piping and cause damage. Even if a probability of 1.2×10^{-5} was taken for rupture of a main steam line, it would be a very minor contributor to pipe failure probability used in this study and thus can be neglected as a significant path for radioactivity releases.

One other probability of interest is the probability of a turbine missile striking the spent fuel storage pool in the PWR or BWR. The highest strike probability estimated by Bush (~4×10^{-3}) was for the PWR. Examination of the PWR layout of interest to this study indicated that the spent fuel pool could be struck only by higher trajectory missiles entering from above the pool; thus the use of this highest estimated strike probability could be overly conservative. Compensating slightly for this conservatism is the fact that either of the two turbines at the two unit sites could generate missiles to potentially strike the fuel and thus double the strike probability. These factors are taken, however, to be within

[1] Note that the BWR containment structure is not listed. This is so because the number and thickness of concrete walls and barriers including the smaller target area of containment make the probability of missile strike and penetration negligibly low.

the bounds of error that could be associated with such probability estimates. Thus use of 4×10^{-3} as an overall strike probability for the spent fuel pool seems reasonable. Given that the turbine missile enters the spent fuel storage pool, the probability of fuel damage was assumed to be unity. The overall probability for spent fuel damage via this accident event was thus taken to be about (10^{-4}) (4×10^{-3}) $(1) = 4 \times 10^{-7}$ and this value was considered by the study as an incremental probability contribution for those accidents not involving the reactor core.[1]

Thus, the probability that a large radioactivity release could be caused by a turbine missile does not represent a significant contribution to the overall risks from reactor accidents.

5.4.6 OTHER EXTERNAL CAUSES

Some plants are located on the sea shore where the possibility of tidal waves, and waves and high water levels due to hurricanes exist. The plant design in these cases must accommodate the largest waves and water levels that can be expected. Such events were assessed to represent negligible risks.

An area often questioned is the possibility of deliberate human acts to destroy the plant. An investigation of this area has led the study to the following conclusions regarding sabotage:

1. Nuclear plants have inherent characteristics that provide built-in difficulties for successful sabotage efforts.

2. Additional security measures have recently been required at nuclear power plants and others are under consideration.

3. The worst consequences associated with acts of sabotage at reactors are not expected to lead to consequences more severe than the maximum consequences predicted by the study. The expected consequences of successful sabotage are but a small fraction of these maximum consequences.

4. Nuclear power plants appear far less susceptible to sabotage than most other civil or industrial targets.

Because there currently is no comprehensive method for estimating the probability of acts of sabotage directed at any target, the consideration of the level of protection against acts of sabotage is thus quite important. Current USNRC guidelines (Safety Guide 1.17 and proposed Section 73.55, 10 CFR), which are significant improvements over previous security practices, have been substantially implemented at operating reactors. Furthermore, recent studies have produced further recommendations for plant countermeasures to supplement the current security measures. As a result of these recommendations, additional requirements are under consideration. The implementation of these improved requirements should further reduce the probability of successful sabotage.

With the implementation of current security measures, it appears that the probability of successful sabotage is low, and further reductions in probability can be anticipated in the future.

5.5 RISKS FROM ACCIDENTAL RELEASES

As discussed in Chapter 2, the risks associated with reactor accidents can be expressed in several ways. However, all these expressions require knowledge of the probabilities and consequences of the various accidents considered.

The probabilities of various accidental releases have been discussed in the preceding sections of this chapter. The consequences have been calculated using the consequence model described in Chapter 4 and Appendix VI. This model uses as its input the values from the release histograms described in section 5.2 in combination with the possible weather states and population densities.

The calculation determines the probability and magnitude of seven different consequences. These are early fatalities (those that occur within a year after a potential accident), early illness, thyroid illness, latent cancer fatalities, genetic effects, property damage and land contamination. By integrating over the entire accident spectrum, weighted by the probability of occurrence, the risk can be obtained in one of several forms. The individual health risk is the average number of people per year expected to be affected by a given consequence divided by the population at risk. The societal health risk is the number of people expected to be affected by a particular consequence per year. Societal risk also includes the estimated annual dollar cost expected from reactor accidents. Perhaps

[1] See section 5 of Appendix I.

the most informative outputs of the calculation, however, are the complementary cumulative distribution functions which show the probability of exceeding consequences of a given magnitude as a result of radioactive releases. The following sections describe the results for both types of reactors expressed in all the above ways for each of the consequence types considered.

The probability-consequence relationship shown in these curves and in the ones that follow are based on population and weather distributions applicable to the sites at which the first 100 reactors will be located. Thus, they represent the combined risk from all sites and are not necessarily the correct curves for a given plant on a given site.

For example, a plant on a very low population site would have a different curve than a plant on a very high population site. Therefore, these curves should not be used to estimate the risks at specific sites.

5.5.1 EARLY FATALITIES

The probability of accidents which produce fatalities versus the expected number of fatalities was calculated using the input data previously described. These results are shown in Fig. 5-3 for both the PWR and the BWR. The differences between the curves for the PWR and BWR are less than the uncertainties inherent in the calculational method. Thus Fig. 5-3 also shows a curve which is the average of the two curves for the individual reactors.[1] The uncertainties in the values of the average curve are indicated by the footnote on Fig. 5-3.

As can be seen from the averaged curve, the probability of an accident that results in more than 10 fatalities is predicted to be about 3×10^{-7} per reactor-year. Thus, in 3,000,000 reactor-years of operation in plants of this type, distributed over sites similar to current U.S. sites, one such event would be expected on the average. Accidents involving 100 or more fatalities are predicted to have a probability of about 10^{-7} and would be expected on the average to occur only once in 10 million reactor years of operation. The largest number of fatalities are predicted to be about 3300 and have a probability of about one in a billion (10^{-9}) per reactor-year.

The probability values from Fig. 5-3 can be thought of as being comprised of four contributing factors; the absolute probability of core melt, the relative probability of various radioactive release categories following core melt, the probability of the existing weather conditions and the probability that a particular population density will be exposed.

Since the consequences result only from potential core melt accident sequences, the probability of core melt affects the absolute value of the probability scale but not the shape of the curve. Changes in this probability would principally affect multiplying the scale by a constant factor. The shape of the curve would be principally determined by the other three factors. Thus, the largest consequences involve the simultaneous occurrence of the largest release category, the worst weather, and the wind blowing in the direction of one of the high population density sectors. Since the poorest weather occurs less than 10% of the time, high population densities occur in less than 1% of the sectors, and the largest release occurs in somewhat less than 10% of the core melt cases, the largest consequences would be expected to occur with a probability of less than one in 10,000 following a core melt accident. Since, as indicated in Appendix V, a potential core melt accident has a probability of about 5×10^{-5}, the probability of the largest consequence events is in the range of 10^{-9} per reactor-year as shown in Fig. 5-3.

Additional perspective can be gained on the meaning of the core melt prediction from the considerations listed below. It should be noted these considerations were not used in the study's calculations.

a. Counting commercial and military power reactors, there have been almost 2000 reactor-years of experience with no nuclear accidents affecting the public. This suggests that the likelihood of an accident is less than 10^{-3} per reactor-year.

b. Examination of accident experience in many fields suggests that large accidents occur with much lower frequency than small accidents.

---

[1] In averaging, the two individual curves are weighted to account for the fact that there are about twice as many PWR's as BWR's in the 100 reactors covered by this study.

This can be seen from the many consequence curves shown in Chapter 6 for both man-made and natural events. They show continuous decreases in frequency of occurrence as the consequences increase. This happens because the largest accidents, as is true with many other low probability processes, require the simultaneous occurrence of several unlikely random events.

c. Since power reactors have not yet had even small accidents, or situations that have resulted in abnormally high fuel temperatures, this again suggests that core melting should be much less likely than 10^{-3} per reactor-year and that larger accidents should have an even smaller frequency. It should be noted that there is only a factor of 20 in probability between a value of 10^{-3} and the predicted value of 5×10^{-5} per reactor year.

Based on these arguments it is reasonable to believe that the core melt probability predicted by this study should not be significantly larger.

Given the probability of core melt at about 5×10^{-5} per year, the probability of accidents with fatalities greater than 10 is $3 \times 10^{-7}/5 \times 10^{-5} = 0.006$ that the consequence will be larger than 10 fatalities. Said another way, 1 out of 170 core melt accidents are predicted to cause more than 10 fatalities. Similarly 1 out of 500 core melt accidents are predicted to cause more than 100 fatalities.

The societal risks for early fatalities are obtained from a probability weighted average of the consequences. This average value is 3×10^{-5} deaths per reactor-year and is essentially the same for both types of plants. However, such an average can have real meaning only when it is representative of many repetitive events. While this is not the case for these low probability reactor accidents, the use of such a calculated average can be of some value in comparing reactor accident risks to other societal risks involving accidents. Such comparisons will be made in Chapter 6.

An individual risk could be obtained by dividing the societal risk by the U.S. population. This gives $3 \times 10^{-5}/2 \times 10^{8} \cong 2 \times 10^{-13}$ per person per reactor-year. However, since fatalities are only expected within 25 miles of the reactor site, a more meaningful number may be the individual risk to the approximately 15 million people living within 25 miles of nuclear sites. This gives an average individual risk of $3 \times 10^{-5}/15 \times 10^{6} = 2 \times 10^{-12}$ per person per reactor-year. The individual risk as a function of distance from the reactor is estimated in Appendix VI.

5.5.2 TABULAR SUMMARY OF RESULTS

The previous section, 5.5.1, presented the early fatality consequences as a function of probability for accidents in PWRs and BWRs and also presented an average of the two curves. Similar curves will be presented in the sections which follow for the other consequences. This section summarizes this consequence data in tabular form for the convenience of the reader. Table 5-4 shows the early fatalities, early injuries, property damage, and land area requiring decontamination or relocation of people as a function of probability. Table 5-5 covers latent cancer fatalities, thyroid illness and genetic effects. These tables show probabilities for having consequences greater than the values listed and each consequence is discussed in greater detail in the sections which follow.

5.5.3 EARLY ILLNESSES

Early illness is defined in this study to be those illnesses which require medical attention shortly after the accident; some of these will require continuing treatment. The most important illness in this category is respiratory impairment. Calculations showed that the ratio of early illnesses to early fatalities is approximately 15 in large potential accidents. The probability distribution for illness is shown in Fig. 5-4. Some additional temporary illnesses are discussed in Appendix VI.

5.5.4 LONG-TERM HEALTH EFFECTS

Exposure to even low levels of radiation, in addition to the natural background of radiation that exists, is generally believed to increase the likelihood of certain diseases and to increase certain genetic effects. Since these effects may be evidenced many years after the exposure, they are classed as long-term health effects. These include latent cancer fatalities, genetic defects, and thyroid illness.

5.5.4.1 Latent Cancer Fatalities.

Radiation-induced cancers can cause an increase in the number of other cancer fatalities in the exposed population. The BEIR Report (Ref. 8) considers this question and concludes that an upper bound on the number of such cancers that might occur after the exposure can be obtained by using a linear extrapolation from high exposure data. The study benefited from the advice of a panel of health consultants which unanimously recommended that the linear hypothesis be used only as an upper bound and that a more realistic estimate be used which accounted for the fact that exposure from a reactor accident would be predominantly gamma radiation of low magnitudes delivered at low dose rates.

The panel felt that, although there is not sufficient evidence to justify the use of a threshold dose, there is, however, enough evidence to justify the use of lower dose-response effectiveness applicable to low dose rates and/or low total doses. The assignment of such factors is discussed in Appendix VI and they have been used in the study's calculations.

The effect of this procedure is to lower the overall BEIR report estimates by about a factor of 2. However, the number of cancer fatalities was predicted in the study's consequence model by adding individual cancers on an organ-by-organ basis rather than by basing the number on the whole body dose. In general, this change increased the number by about a factor of two. The overall effect of these two changes was to give a total number of predicted cancers that is equivalent to about 100 cancer fatalities per 10^6 man-rem, based on a whole body dose. Figure 5-5 is a plot of the probability distribution of latent cancer fatalities per year most of which could occur approximately over a period of 10 to 40 years following a potential accident. In the largest accident predicted in the study the 1500 latent cancer fatalities would be distributed over approximately 10 million people. The normal incidence rate of fatal cancer in this population is about 17,000 (Ref. 9) per year. Thus the largest potential accident would represent an increase over the normal rate of 1500/17000, or about 9%. This effect would probably not be measurable statistically because of the large variations in the normal rate.

The probability of 500 latent cancer fatalities/yr or more is about 10^{-7} per reactor-year. Thus 80% of core melts are predicted to cause less than 500 latent cancers/yr.

5.5.4.2 Thyroid Nodules

It has been observed that radiation exposure of the thyroid gland increases the likelihood of thyroid nodules. On the average, considering different age groups, about 1/3 of all nodules would be malignant. Both types of nodules can be medically treated with good success. In this study, it has been assumed that 10% of the malignant nodules will have a fatal outcome and this number has been added to the number of latent cancer fatalities. Figure 5-6 presents the incidence rate for all nodules. This rate would be expected to presist from about 10 to 40 years after the accident on the average. In the largest accident predicted in this study, the 8000 cases per year would be distributed over about 10 million people. The normal annual incidence rate of nodules in this population is about 8000 per year. Thus the largest accident would approximately double the normal incidence; this effect would be detectable in the population at risk.

As noted in Appendix VI hypothyroidism may also result from irradiation in some cases. Hypothroidism is a deficiency of thyroid activity which occurs spontanously and may be induced by irradiation of the thyroid. Hyperthyroidism (overactivity of the thyroid gland) and thyroid cancer are often treated by administering to the patient a dose of iodine-131 which, taken up by the thyroid, reduces the thyroid function and destroys the cancerous cells. A hypothyroid person is normally prescribed replacement thyroid hormones which are taken orally and are inexpensive, effective and safe. Neither the BEIR report or UNSCEAR provide risk estimates for hypothyroidism. Based on the limited data presently available and on the fact that it may not be applicable to the general population as summarized in Appendix VI, the study has roughly estimated that the number of cases of hypothroidism may be of the same order as the number of nodules. A more definite estimate must await further work.

5.5.4.3 Genetic Effects

Genetic mutations can occur spontaneously, from unknown causes, or can be induced by a variety of physical or chemical agents, one of which is ionizing radiation. The effects of

mutations can be very obvious, e.g. albinism, or detectable only by laboratory tests; they can be so slight as to be neither incapacitating nor disfiguring or so severe as to produce pronounced life shortening in a small percentage of the cases. The effect of radiation is to increase the mutation rate but genetic disorders that would arise from radiation-induced mutation would not differ from those that have been occurring naturally for as long as man has existed. The increases in genetically caused diseases expected for a particular exposure have been summarized in Appendix VI based on estimates from several sources.

The probability distribution for the number of genetic effects that might occur are given in Fig. 5-7. In this curve the genetic effects per year apply to the first generation and would occur over about a 30 year period. Additional genetic effects could also occur in later generations. The total effect can be calculated approximately by assuming that the first generation rate would persist for about 150 years. The number of cases of genetic defects that could be produced by the largest accident predicted in this study is 190/yr. Since the normal incidence rate of genetic effects in the approximately 10 million people affected is approximately 8000 per year, the 190 cases per year would represent an increase in the normal rate of approximately 2%.

5.5.5 PROPERTY DAMAGE

The property damage model provides an approximate estimate of the more significant societal costs that might occur as the result of a potential accident in a nuclear power plant. Although the damage that might occur is called property damage, it must be recognized that no property located off the reactor site would be physically damaged; rather it may become sufficiently contaminated with radioactive material so that its usefulness is temporarily or permanently impaired. This means that before it would become useful again, the radioactivity must decay or weather away until it reaches acceptable levels or decontamination action must be taken to achieve these levels. The property damage model considers the effects of both decay and decontamination.

The potential costs to society considered in the model are accumulated from five sources. They are the cost of 1) evacuating people to reduce their exposures to the radioactivity released, 2) the temporary relocation of people who may be in an area that is contaminated to higher than acceptable levels for long-term occupation, 3) decontamination of this area, 4) property that cannot reasonably be decontaminated and 5) agricultural products for a growing season, if the contamination levels were to be high enough to prevent their use. The treatment of each of these effects is discussed in detail in Appendix VI.

The major contributor to the overall cost would be from those areas where reasonable decontamination procedures could not reduce levels of radioactivity to acceptable levels of dose. In this study an acceptable dose level was chosen to be 25 rem in 30 years for urban areas and 10 rem in 30 years for areas where the population density is low. These values are based on concepts contained in the Federal Radiation Council (Ref. 10,11) and British Medical Research Council (Ref. 12) publications which state that the 10 or 15 rem reference dose is one below which countermeasures are unlikely to be justified. When a radiation dose appears likely to exceed the reference dose, a balance should be achieved between the risk to the community from relocation versus the risk due to some increased exposure.

The dollar costs charged for permanent relocation are on the basis of $17,000/capita to account for value of property, land and relocation costs. A somewhat larger land area than the relocation area will remain habitable, but will require some decontamination. This decontamination can range from a simple washing (which may yield decontamination factors of 2) to more thorough procedures which will yield a decontamination factor of about 20. The model assumes that, should an accident occur, such measures will be regarded as reasonable and will be implemented where appropriate, thus reducing the area that cannot be inhabited. The cost for thorough decontamination is estimated to be about 10% of the value of the property and is included in the overall property damage estimate.

Agricultural costs are assessed by determining the fraction of land (in each state) that is in agricultural production and determining the value of any lost crops. Milk production for a few weeks to a few months is very sensitive to radioiodine contamination so it is treated by a separate calculation. Agricultural costs are a minor contributor to overall property damage.

The predicted property damage costs are shown in Fig. 5-8. The curve shows that 80% of all core melt cases would have damage costs of less than $300 million and that 99% would have costs less than $4 billion. These curves are considered to represent a conservative estimate of the costs because the effects of wind direction change and wind shear are not accounted for by the consequence model. The inclusion of these effects would tend to reduce the land area that might be contaminated to higher than acceptable levels.

Figure 5-9 shows the probability distribution of land area affected for the two conditions described above. The higher curve is an area from which people would not be relocated but in which decontamination would be required. The lower curve is an area from which people would have to be relocated. Although a portion of this area would become useful after decontamination, the dollar damage estimates incorporated the total value of structures and land within this area.

The areas in Fig. 5-9 are calculated on the basis of the acceptable level of dose for continued occupation of 25 rem in 30 years. As is shown in Appendix VI, on the average, if this level were to be increased to 50 rem, the areas shown in these curves would be reduced by a factor of 4; however, this would cause about a 10% increase in latent cancers and genetic effects. Similarly, a decrease to 10 rem would increase the area by a factor of 2.5 and decrease the latent cancers and genetic effects by about 10%.

It can be seen from Fig. 5-9, that in 80% of all potential core melt accidents, the area that might require relocation is less than 20 square miles and the area requiring decontamination is less than 400 square miles.

It can be seen from Fig. 5-9, that in 80% of all potential core melt accidents, the area that might require relocation is less than 20 square miles and the area requiring decontamination is less than 400 square miles.

In order to keep radioactivity out of the human food chain it would be necessary to impound certain agricultural products over a somewhat larger area. The most sensitive agricultural product is milk and the area over which milk would have to be monitored for a few weeks to a few months is about 5 times larger than the decontamination curve. The costs associated with these agricultural products is less than 5% of the total cost.

The effects of contamination of water supplies have not been considered in detail in the study. In the case of streams and rivers the effect of contamination of water to levels of radioactivity above drinking water tolerances would be to restrict use of the water during the period that contaminated water would flow past water supply intakes. This type of control procedure should have small effects on public health. Contamination of a water supply reservoir would require that an alternate supply be used until the radioactive levels decayed to drinking water levels or until the city water supply can adequately filter to achieve acceptable levels. Contamination of a large lake or reservoir that represented the major water supply to a city would require restrictions on its use until levels were suitably low or until proper filtering could be implemented. It is believed that the property damage values calculated for land would cover the costs of additional water filtration when it is required.

5.6 ACCIDENT RISKS DUE TO 100 NUCLEAR POWER PLANTS

The risks reported in the previous sections were on a per plant basis. An estimate of the total risk to society of 100 reactors operating at the currently assigned sites can be obtained by multiplying the PWR and the BWR curves by the number of each type of plant in the population of 100 and then adding the result. However, the differences in the calculation of the risks involved in the two plants are well within the uncertainties involved in the analysis, so the total risk has been obtained by taking the weighted average of the PWR and BWR results and multiplying the result by 100.

It must be recognized that there are certain assumptions involved in expanding the results to include 100 reactors which require discussion. Such a procedure assumes that all reactors in the population have the same overall risk. As discussed in Chapter 2, technologies typically show improvements in their safety as a function of time. As pointed out in Chapter 1, since about two thirds of the first 100 large plants will be of newer vintage than the plants studied, it would be expected that this study has somewhat over-predicted the risk. Furthermore, improvements in reliability and safety can reasonably be

anticipated during the next decade or more as a result of operating experience and improved designs. These improvements (some of which are already incorporated in newer plants) make it inappropriate to extend the results of this study to more than 100 plants or beyond a 5-10 year period.

Using the process described above, the probability distributions for various accident consequences similar to those shown earlier for 1 reactor can be obtained for 100 reactors. Table 5-6 shows the approximate annual societal and individual risks due to potential nuclear plant accidents for 100 reactors located at the 68 sites used in the study. Tables 5-7 and 5-8 present the various consequences vs. probability for 100 reactors. These show probabilities for having consequences greater than the values listed. Figures 5-10 - 5-16 show the various consequence curves.

References

1. UCLA-ENG-7516, Hseih, T. et al., "On the Average Probability Distribution of Peak Ground Acceleration in the U.S. Continent Due to Strong Earthquakes," March 1975.

2. Newmark, N. M., "Probability of Predicted Seismic Damage in Relation to Nuclear Reactor Facility Design (Draft)," September 1975.

3. Brazee, R. J., "Attenuation of MMI with Distance for the United States East of 106°W," Earthquake Note, Vol. 43, No. 1, pp 41-52, March 1972.

4. Cornell, C. A. and Hans A. Mertz, "Seismic Risk Analysis of Boston," ASCE Meeting, April 22-24, 1974.

5. Doan, P. L., "Tornado Considerations for Nuclear Power Plant Structures Including the Spent Fuel Storage Pool," Nuclear Safety, Vol. II, No. 4, July-August, 1970.

6. USAEC Draft Regulatory Guide 1.XX, "Design Basis Tornado for Nuclear Power Plants," Oct. 11, 1973.

7. Bush, Spencer H., "Probability of Damage to Nuclear Components Due to Turbine Failure," Nuclear Safety, Vol. 14, No. 3, May-June 1973.

8. "The Effects on Populations of Exposure to Low Levels of Ionizing Radiation," Report of the Advisory Committee on the Biological Effects of Ionizing Radiations, Division of Medical Sciences, National Academy of Sciences, National Research Council, November 1972.

9. American Cancer Society "75 Cancer Facts and Figures" (1974).

10. Federal Radiation Council, 1964, Background Material for the Development of Radiation Protection Standards, FRC Staff Report No. 5.

11. Federal Radiation Council, 1965, Background Material for the Development of Protective Action Guides for Strontium-89, Acentium-90, and Cesium-137, FRC Staff Report No. 7.

12. Medical Research Council, 1975, Criteria for Controlling Radiation Doses to the Public After Accidental Escapes of Radioactive Material, Her Majesty's Stationery Office, London.

TABLE 5-1 SUMMARY OF ACCIDENTS INVOLVING CORE

RELEASE CATEGORY	PROBABILITY per Reactor-Yr	TIME OF RELEASE (Hr)	DURATION OF RELEASE (Hr)	WARNING TIME FOR EVACUATION (Hr)	ELEVATION OF RELEASE (Meters)	CONTAINMENT ENERGY RELEASE (10^6 Btu/Hr)	FRACTION OF CORE INVENTORY RELEASED[a]							
							Xe-Kr	Org. I	I	Cs-Rb	Te-Sb	Ba-Sr	Ru[b]	La[c]
PWR 1	9×10^{-7}	2.5	0.5	1.0	25	520[d]	0.9	6×10^{-3}	0.7	0.4	0.4	0.05	0.4	3×10^{-3}
PWR 2	8×10^{-6}	2.5	0.5	1.0	0	170	0.9	7×10^{-3}	0.7	0.5	0.3	0.06	0.02	4×10^{-3}
PWR 3	4×10^{-6}	5.0	1.5	2.0	0	6	0.8	6×10^{-3}	0.2	0.2	0.3	0.02	0.03	3×10^{-3}
PWR 4	5×10^{-7}	2.0	3.0	2.0	0	1	0.6	2×10^{-3}	0.09	0.04	0.03	5×10^{-3}	3×10^{-3}	4×10^{-4}
PWR 5	7×10^{-7}	2.0	4.0	1.0	0	0.3	0.3	2×10^{-3}	0.03	9×10^{-3}	5×10^{-3}	1×10^{-3}	6×10^{-4}	7×10^{-5}
PWR 6	6×10^{-6}	12.0	10.0	1.0	0	N/A	0.3	2×10^{-3}	8×10^{-4}	8×10^{-4}	1×10^{-3}	9×10^{-5}	7×10^{-5}	1×10^{-5}
PWR 7	4×10^{-5}	10.0	10.0	1.0	0	N/A	6×10^{-3}	2×10^{-5}	2×10^{-5}	1×10^{-5}	2×10^{-5}	1×10^{-6}	1×10^{-6}	2×10^{-7}
PWR 8	4×10^{-5}	0.5	0.5	N/A	0	N/A	2×10^{-3}	5×10^{-6}	1×10^{-4}	5×10^{-4}	1×10^{-6}	1×10^{-8}	0	0
PWR 9	4×10^{-4}	0.5	0.5	N/A	0	N/A	3×10^{-6}	7×10^{-9}	1×10^{-7}	6×10^{-7}	1×10^{-9}	1×10^{-11}	0	
BWR 1	1×10^{-6}	2.0	2.0	1.5	25	130	1.0	7×10^{-3}	0.40	0.40	0.70	0.05	0.5	5×10^{-3}
BWR 2	6×10^{-6}	30.0	3.0	2.0	0	30	1.0	7×10^{-3}	0.90	0.50	0.30	0.10	0.03	4×10^{-3}
BWR 3	2×10^{-5}	30.0	3.0	2.0	25	20	1.0	7×10^{-3}	0.10	0.10	0.30	0.01	0.02	3×10^{-3}
BWR 4	2×10^{-6}	5.0	2.0	2.0	25	N/A	0.6	7×10^{-4}	8×10^{-4}	5×10^{-3}	4×10^{-3}	6×10^{-4}	6×10^{-4}	1×10^{-4}
BWR 5	1×10^{-4}	3.5	5.0	N/A	150	N/A	5×10^{-4}	2×10^{-9}	6×10^{-11}	4×10^{-9}	8×10^{-12}	8×10^{-14}	0	0

(a) A discussion of the isotopes used in the study is found in Appendix VI. Background on the isotope groups and release mechanisms is found in Appendix VII.

(b) Includes Mo, Rh, Tc, Co.

(c) Includes Nd, Y, Ce, Pr, La, Nb, Am, Cm, Pu, Np, Zr.

(d) A lower energy release rate than this value applies to part of the period over which the radioactivity is being released. The effect of lower energy release rates on consequences is found in Appendix VI.

TABLE 5-2 PWR DOMINANT ACCIDENT SEQUENCES vs. RELEASE CATEGORIES

RELEASE CATEGORIES							Core Melt	No Core Melt	
	1	2	3	4	5	6	7	8	9
LARGE LOCA A	$AB\text{-}\alpha\ 1\times10^{-11}$ $AF\text{-}\alpha\ 1\times10^{-10}$ $ACD\text{-}\alpha\ 5\times10^{-11}$ $AG\text{-}\alpha\ 9\times10^{-11}$	$AB\text{-}\gamma\ 1\times10^{-10}$ $AB\text{-}\delta\ 4\times10^{-11}$ $AHF\text{-}\gamma\ 2\times10^{-11}$	$AD\text{-}\alpha\ 2\times10^{-8}$ $AH\text{-}\alpha\ 1\times10^{-8}$ $AF\text{-}\delta\ 1\times10^{-8}$ $AG\text{-}\delta\ 9\times10^{-9}$	$ACD\text{-}\beta\ 1\times10^{-11}$	$AD\text{-}\beta\ 4\times10^{-9}$ $AH\text{-}\beta\ 3\times10^{-9}$	$AB\text{-}\varepsilon\ 1\times10^{-9}$ $AHF\text{-}\varepsilon\ 1\times10^{-10}$ $ADF\text{-}\varepsilon\ 2\times10^{-10}$	$AD\text{-}\varepsilon\ 2\times10^{-6}$ $AH\text{-}\varepsilon\ 1\times10^{-6}$	$A\text{-}\beta\ 2\times10^{-7}$	$A\ 1\times10^{-4}$
A Probabilities	2×10^{-9}	1×10^{-8}	1×10^{-7}	1×10^{-8}	4×10^{-8}	3×10^{-7}	3×10^{-6}	1×10^{-5}	1×10^{-4}
SMALL LOCA S_1	$S_1B\text{-}\alpha\ 3\times10^{-11}$ $S_1CD\text{-}\alpha\ 7\times10^{-11}$ $S_1F\text{-}\alpha\ 3\times10^{-10}$ $S_1G\text{-}\alpha\ 3\times10^{-10}$	$S_1B\text{-}\gamma\ 4\times10^{-10}$ $S_1B\text{-}\delta\ 1\times10^{-10}$ $S_1HF\text{-}\gamma\ 6\times10^{-11}$	$S_1D\text{-}\alpha\ 3\times10^{-8}$ $S_1H\text{-}\alpha\ 3\times10^{-8}$ $S_1F\text{-}\delta\ 3\times10^{-8}$ $S_1G\text{-}\delta\ 3\times10^{-8}$	$S_1CD\text{-}\beta\ 1\times10^{-11}$	$S_1H\text{-}\beta\ 5\times10^{-9}$ $S_1D\text{-}\beta\ 6\times10^{-9}$	$S_1DF\text{-}\varepsilon\ 3\times10^{-10}$ $S_1B\text{-}\varepsilon\ 2\times10^{-9}$ $S_1HF\text{-}\varepsilon\ 4\times10^{-10}$	$S_1D\text{-}\varepsilon\ 3\times10^{-6}$ $S_1H\text{-}\varepsilon\ 3\times10^{-6}$	$S_1\text{-}\beta\ 6\times10^{-7}$	$S_1\ 3\times10^{-4}$
S_1 Probabilities	3×10^{-9}	2×10^{-8}	2×10^{-7}	3×10^{-8}	8×10^{-8}	6×10^{-7}	6×10^{-6}	3×10^{-5}	3×10^{-4}
SMALL LOCA S_2	$S_2B\text{-}\alpha\ 1\times10^{-10}$ $S_2F\text{-}\alpha\ 1\times10^{-9}$ $S_2CD\text{-}\alpha\ 2\times10^{-10}$ $S_2G\text{-}\alpha\ 9\times10^{-10}$ $S_2C\text{-}\alpha\ 2\times10^{-8}$	$S_2B\text{-}\gamma\ 1\times10^{-9}$ $S_2HF\text{-}\gamma\ 2\times10^{-10}$ $S_2B\text{-}\delta\ 4\times10^{-10}$	$S_2D\text{-}\alpha\ 9\times10^{-8}$ $S_2H\text{-}\alpha\ 6\times10^{-8}$ $S_2F\text{-}\delta\ 1\times10^{-7}$ $S_2C\text{-}\delta\ 2\times10^{-6}$ $S_2G\text{-}\delta\ 9\times10^{-8}$	$S_2DG\text{-}\beta\ 1\times10^{-12}$	$S_2D\text{-}\beta\ 2\times10^{-8}$ $S_2H\text{-}\beta\ 1\times10^{-8}$	$S_2B\text{-}\varepsilon\ 8\times10^{-9}$ $S_2CD\text{-}\varepsilon\ 2\times10^{-8}$ $S_2HF\text{-}\varepsilon\ 1\times10^{-9}$	$S_2D\text{-}\varepsilon\ 9\times10^{-6}$ $S_2H\text{-}\varepsilon\ 6\times10^{-6}$		
S_2 Probabilities	1×10^{-7}	3×10^{-7}	3×10^{-6}	3×10^{-7}	3×10^{-7}	2×10^{-6}	2×10^{-5}		
REACTOR VESSEL RUPTURE - R	$RC\text{-}\alpha\ 2\times10^{-12}$	$RC\text{-}\gamma\ 3\times10^{-11}$ $RF\text{-}\delta\ 1\times10^{-11}$ $RC\text{-}\delta\ 1\times10^{-12}$	$R\text{-}\alpha\ 1\times10^{-9}$				$R\text{-}\varepsilon\ 1\times10^{-7}$		
R Probabilities	2×10^{-11}	1×10^{-10}	1×10^{-9}	2×10^{-10}	1×10^{-9}	1×10^{-8}	1×10^{-7}		
INTERFACING SYSTEMS LOCA (CHECK VALVE) - V		$V\ 4\times10^{-6}$							
V Probabilities	4×10^{-7}	4×10^{-6}	4×10^{-7}	4×10^{-8}					
TRANSIENT EVENT - T	$TMLB'\text{-}\alpha\ 3\times10^{-8}$	$TMLB'\text{-}\gamma\ 7\times10^{-7}$ $TMLB'\text{-}\delta\ 2\times10^{-6}$	$TML\text{-}\alpha\ 6\times10^{-8}$ $TKQ\text{-}\alpha\ 3\times10^{-8}$ $TKMQ\text{-}\alpha\ 1\times10^{-8}$		$TML\text{-}\beta\ 3\times10^{-10}$ $TKQ\text{-}\beta\ 3\times10^{-10}$	$TMLB'\text{-}\varepsilon\ 6\times10^{-7}$	$TML\text{-}\varepsilon\ 6\times10^{-6}$ $TKQ\text{-}\varepsilon\ 3\times10^{-6}$ $TKMQ\text{-}\varepsilon\ 1\times10^{-6}$		
T Probabilities	3×10^{-7}	3×10^{-6}	4×10^{-7}	7×10^{-8}	2×10^{-7}	2×10^{-6}	1×10^{-5}		
(Σ) SUMMATION OF ALL ACCIDENT SEQUENCES PER RELEASE CATEGORY									
MEDIAN (50% VALUE)	9×10^{-7}	8×10^{-6}	4×10^{-6}	5×10^{-7}	7×10^{-7}	6×10^{-6}	4×10^{-5}	4×10^{-5}	4×10^{-4}
LOWER BOUND (5% VALUE)	9×10^{-8}	8×10^{-7}	6×10^{-7}	9×10^{-8}	2×10^{-7}	2×10^{-6}	1×10^{-5}	4×10^{-6}	4×10^{-5}
UPPER BOUND (95% VALUE)	9×10^{-6}	8×10^{-5}	4×10^{-5}	5×10^{-6}	4×10^{-6}	2×10^{-5}	2×10^{-4}	4×10^{-4}	4×10^{-3}

Note: The probabilities for each release category for each event tree and the Σ for all accident sequences are the median values of the dominant accident sequences summed by Monte Carlo simulation plus a 10% contribution from the adjacent release category probability.

KEY TO TABLE 5-2 ON FOLLOWING PAGE

KEY TO PWR ACCIDENT SEQUENCE SYMBOLS

A - Intermediate to large LOCA.

B - Failure of electric power to ESFs.

B' - Failure to recover either onsite or offsite electric power within about 1 to 3 hours following an initiating transient which is a loss of offsite AC power.

C - Failure of the containment spray injection system.

D - Failure of the emergency core cooling injection system.

F - Failure of the containment spray recirculation system.

G - Failure of the containment heat removal system.

H - Failure of the emergency core cooling recirculation system.

K - Failure of the reactor protection system.

L - Failure of the secondary system steam relief valves and the auxiliary feedwater system.

M - Failure of the secondary system steam relief valves and the power conversion system.

Q - Failure of the primary system safety relief valves to reclose after opening.

R - Massive rupture of the reactor vessel.

S_1 - A small LOCA with an equivalent diameter of about 2 to 6 inches.

S_2 - A small LOCA with an equivalent diameter of about 1/2 to 2 inches.

T - Transient event.

V - LPIS check valve failure.

α - Containment rupture due to a reactor vessel steam explosion.

β - Containment failure resulting from inadequate isolation of containment openings and penetrations.

γ - Containment failure due to hydrogen burning.

δ - Containment failure due to overpressure.

ϵ - Containment vessel melt-through.

KEY TO TABLE 5-2

TABLE 5-3 BWR DOMINANT ACCIDENT SEQUENCES OF EACH EVENT TREE vs. RELEASE CATEGORY

	Core Melt				No Core Melt
	RELEASE CATEGORIES				
	1	2	3	4	5
LARGE LOCA DOMINANT ACCIDENT SEQUENCES (A)	AE-α 2×10^{-9} AJ-α 1×10^{-10} AHI-α 1×10^{-10} AI-α 1×10^{-10}	AE-γ′ 3×10^{-8} AE-β 1×10^{-8} AJ-γ′ 2×10^{-9} AI-γ′ 2×10^{-9} AHI-γ′ 2×10^{-9}	AE-γ 1×10^{-7} AJ-γ 1×10^{-8} AI-γ 1×10^{-8} AHI-γ 1×10^{-8}	AGJ-δ 6×10^{-11} AEG-δ 7×10^{-10} AGHI-δ 6×10^{-11}	A 1×10^{-4}
A Probabilities	8×10^{-9}	6×10^{-8}	2×10^{-7}	2×10^{-8}	1×10^{-4}
SMALL LOCA DOMINANT ACCIDENT SEQUENCES (S_1)	S_1E-α 2×10^{-9} S_1J-α 3×10^{-10} S_1I-α 4×10^{-10} S_1HI-α 4×10^{-10}	S_1E-γ′ 4×10^{-8} S_1E-β 1×10^{-8} S_1J-γ′ 7×10^{-9} S_1I-γ′ 7×10^{-9} S_1HI-γ′ 6×10^{-9}	SE-γ 1×10^{-7} S_1C-γ 3×10^{-8} S_1I-γ 4×10^{-8} S_1HI-γ 2×10^{-8} S_1C-γ 3×10^{-9}	S_1GJ-δ 2×10^{-10} S_1GE-δ 2×10^{-10} S_1EI-ε 1×10^{-10} S_1GHI-δ 2×10^{-10}	
S_1 Probabilities	1×10^{-8}	9×10^{-8}	2×10^{-7}	2×10^{-8}	
SMALL LOCA DOMINANT ACCIDENT SEQUENCES (S_2)	S_2J-α 1×10^{-9} S_2I-α 1×10^{-9} S_2HI-α 1×10^{-9} S_2E-α 5×10^{-10}	S_2E-γ′ 1×10^{-8} S_2E-β 4×10^{-9} S_2J-γ′ 2×10^{-8} S_2I-γ′ 2×10^{-8} S_2HI-γ′ 2×10^{-8}	S_2E-γ 4×10^{-8} S_2J-γ 8×10^{-8} S_2I-γ 9×10^{-8} S_2HI-γ 9×10^{-8} S_2C-γ 8×10^{-9}	S_2CG-δ 6×10^{-11} S_2GHI-δ 6×10^{-10} S_2EG-δ 3×10^{-10} S_2GJ-δ 6×10^{-10} S_2GI-δ 2×10^{-10}	
S_2 Probabilities	2×10^{-8}	1×10^{-7}	4×10^{-7}	4×10^{-8}	
TRANSIENT DOMINANT ACCIDENT SEQUENCES (T)	TW-α 2×10^{-7} TC-α 1×10^{-7} TQUV-α 5×10^{-9}	TW-γ′ 3×10^{-6} TQUV-γ′ 8×10^{-8}	TW-γ 1×10^{-5} TC-γ 1×10^{-5} TQUV-γ 4×10^{-7}		
T Probabilities	1×10^{-6}	6×10^{-6}	2×10^{-5}	2×10^{-6}	
PRESSURE VESSEL RUPTURE ACCIDENTS (R)		P.V. RUPT. 1×10^{-9} Oxidizing Atmosphere	P.V. RUPT. 1×10^{-7} Non-oxidizing Atmosphere		
R Probabilities	2×10^{-9}	2×10^{-8}	1×10^{-7}	1×10^{-8}	
SUMMATION OF ALL ACCIDENT SEQUENCES PER RELEASE CATEGORIES					
MEDIAN (50% VALUE)	1×10^{-6}	6×10^{-6}	2×10^{-5}	2×10^{-6}	1×10^{-4}
LOWER BOUND (5% VALUE)	1×10^{-7}	1×10^{-6}	5×10^{-6}	5×10^{-7}	1×10^{-5}
UPPER BOUND (95% VALUE)	6×10^{-6}	3×10^{-5}	8×10^{-5}	1×10^{-5}	1×10^{-3}

NOTE: The probabilities for each release category for each event tree and the Σ for all accident sequences are the median values of the dominant accident sequences summed by Monte Carlo simulation plus a 10% contribution from the adjacent release category probability.

KEY TO TABLE 5-3 ON FOLLOWING PAGE

KEY TO BWR ACCIDENT SEQUENCE SYMBOLS

A - Rupture of reactor coolant boundary with an equivalent diameter of greater than six inches.

B - Failure of electric power to ESFs.

C - Failure of the reactor protection system.

D - Failure of vapor suppression.

E - Failure of emergency core cooling injection.

F - Failure of emergency core cooling functionability.

G - Failure of containment isolation to limit leakage to less than 100 volume per cent per day.

H - Failure of core spray recirculation system.

I - Failure of low pressure recirculation system.

J - Failure of high pressure service water system.

M - Failure of safety/relief valves to open.

P - Failure of safety/relief valves to reclose after opening.

Q - Failure of normal feedwater system to provide core make-up water.

S_1 - Small pipe break with an equivalent diameter of about 2"-6".

S_2 - Small pipe break with an equivalent diameter of about 1/2"-2".

T - Transient event.

U - Failure of HPCI or RCIC to provide core make-up water.

V - Failure of low pressure ECCS to provide core make-up water.

W - Failure to remove residual core heat.

α - Containment failure due to steam explosion in vessel.

β - Containment failure due to steam explosion in containment.

γ - Containment failure due to overpressure - release through reactor building.

γ' - Containment failure due to overpressure - release direct to atmosphere.

δ - Containment isolation failure in drywell.

ε - Containment isolation failure in wetwell.

ζ - Containment leakage greater than 2400 volume per cent per day.

η - Reactor building isolation failure.

θ - Standby gas treatment system failure.

KEY TO TABLE 5-3

TABLE 5-4 CONSEQUENCES OF REACTOR ACCIDENTS FOR VARIOUS PROBABILITIES FOR ONE REACTOR

Chance per Reactor-Year	Consequences				
	Early Fatalities	Early Illness	Total Property Damage 10^9	Decontamination Area ∿ Square Miles	Relocation Area Square Miles
One in 20,000[a]	<1.0	<1.0	<0.1	<0.1	<0.1
One in 1,000,000	<1.0	300	0.9	2000	130
One in 10,000,000	110	3000	3	3200	250
One in 100,000,000	900	14,000	8	-	290
One in 1,000,000,000	3300	45,000	14	-	-

(a)This is the predicted chance of core melt per reactor year.

TABLE 5-5 CONSEQUENCES OF REACTOR ACCIDENTS FOR VARIOUS PROBABILITIES FOR ONE REACTOR

Chance Per Reactor-Year	Consequences		
	Latent Cancer[b] Fatalities (per year)	Thyroid Nodules[b] (per year)	Genetic Effects[c] (per year)
One in 20,000[a]	<1.0	<1.0	<1.0
One in 1,000,000	170	1400	25
One in 10,000,000	460	3500	60
One in 100,000,000	860	6000	110
One in 1,000,000,000	1500	8000	170
Normal Incidence	17,000	8000	8000

(a) This is the predicted chance of core melt per reactor year.
(b) This rate would occur approximately in the 10 to 40 year period following a potential accident.
(c) This rate would apply to the first generation born after a potential accident. Subsequent generations would experience effects at a lower rate.

TABLE 5-6 APPROXIMATE AVERAGE SOCIETAL AND INDIVIDUAL RISK PROBABILITIES PER YEAR FROM POTENTIAL NUCLEAR PLANT ACCIDENTS[a]

Consequence	Societal	Individual
Early Fatalities[b]	3×10^{-3}	2×10^{-10}
Early Illness[b]	2×10^{-1}	1×10^{-8}
Latent Cancer Fatalities[c]	7×10^{-2}/yr	3×10^{-10}/yr
Thyroid Nodules[c]	7×10^{-1}/yr	3×10^{-9}/yr
Genetic Effects[d]	1×10^{-2}/yr	7×10^{-11}/yr
Property Damage ($)	2×10^{6}	——

(a) Based on 100 reactors at 68 current sites.

(b) The individual risk value is based on the 15 million people living in the general vicinity of the first 100 nuclear power plants.

(c) This value is the rate of occurrence per year for about a 30-year period following a potential accident. The individual rate is based on the total U.S. population.

(d) This value is the rate of occurrence per year for the first generation born after a potential accident; subsequent generations would experience effects at a lower rate. The individual rate is based on the total U.S. population.

TABLE 5-7 CONSEQUENCES OF REACTOR ACCIDENTS FOR VARIOUS PROBABILITIES FOR 100 REACTORS

	Consequences				
Chance Per Year	Early Fatalities	Early Illness	Total Property Damage $10^9	Decontamination Area Square Miles	Relocation Area Square Miles
One in 200[a]	<1.0	<1.0	<0.1	<0.1	<0.1
One in 10,000	<1.0	300	0.9	2000	130
One in 100,000	110	300	3	3200	250
One in 1,000,000	900	14000	8	(b)	290
One in 10,000,000	3300	45000	14	(b)	(b)

(a) This is the predicted chance per year of core melt considering 100 reactors.
(b) No change from previously listed values.

TABLE 5-8 CONSEQUENCES OF REACTOR ACCIDENTS FOR VARIOUS PROBABILITIES FOR 100 REACTORS

Chance Per Year	Consequences		
	Latent Cancer Fatalities[b] (per year)	Thyroid Nodules[b] (per year)	Genetic Effects[c] (per year)
One in 200[a]	<1.0	<1.0	<1.0
One in 10,000	170	1400	25
One in 100,000	460	3500	60
One in 1,000,000	860	6000	110
One in 10,000,000	1500	8000	170
Normal Incidence	17,000	8000	8000

(a) This is the predicted chance per year of core melt for 100 reactors.

(b) This rate would occur approximately in the 10 to 40 year period after a potential accident.

(c) This rate would apply to the first generation born after the accident. Subsequent generations would experience effects at decreasing rates.

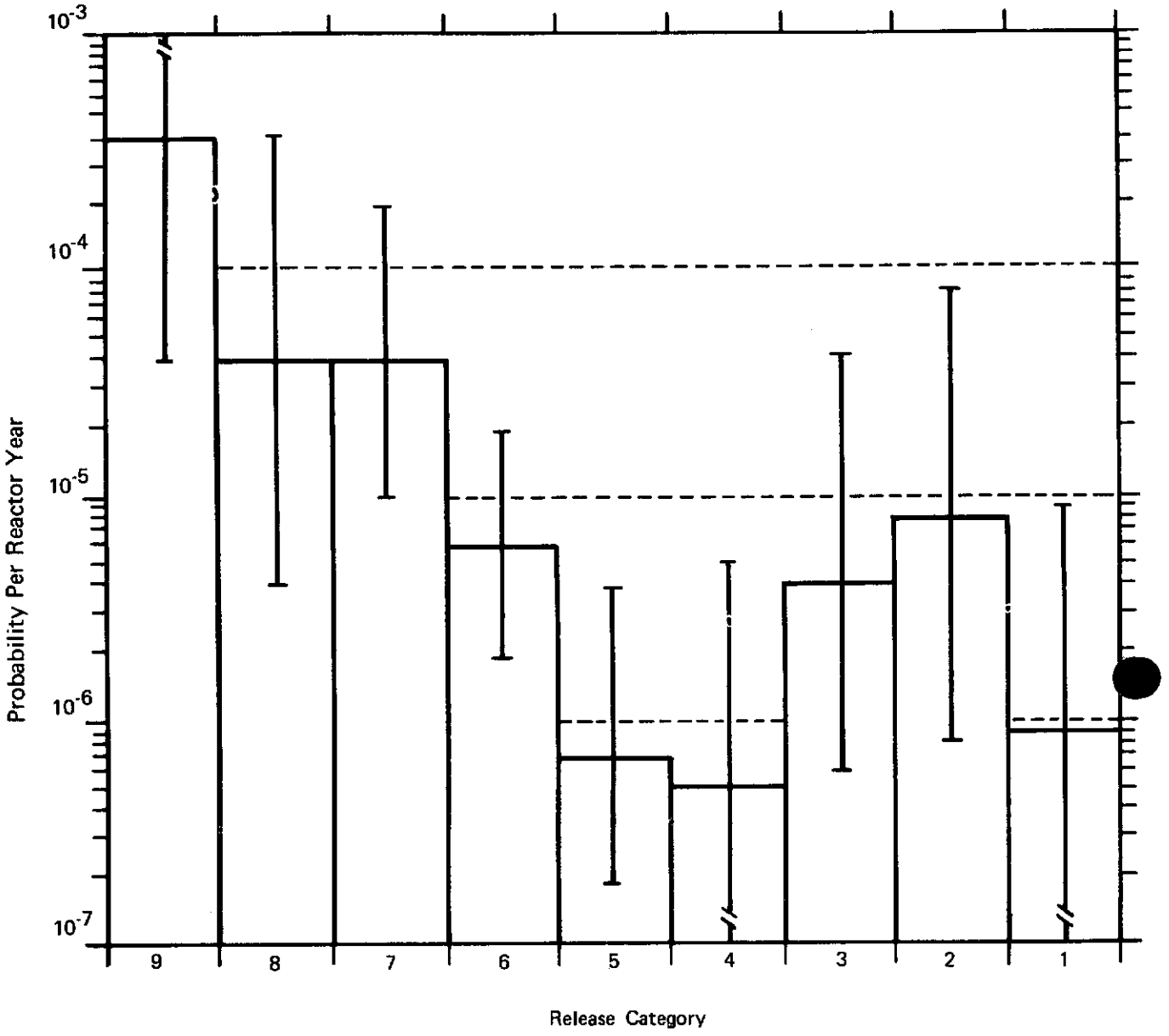


FIGURE 5-1 Histogram of PWR Radioactive Release Probabilities

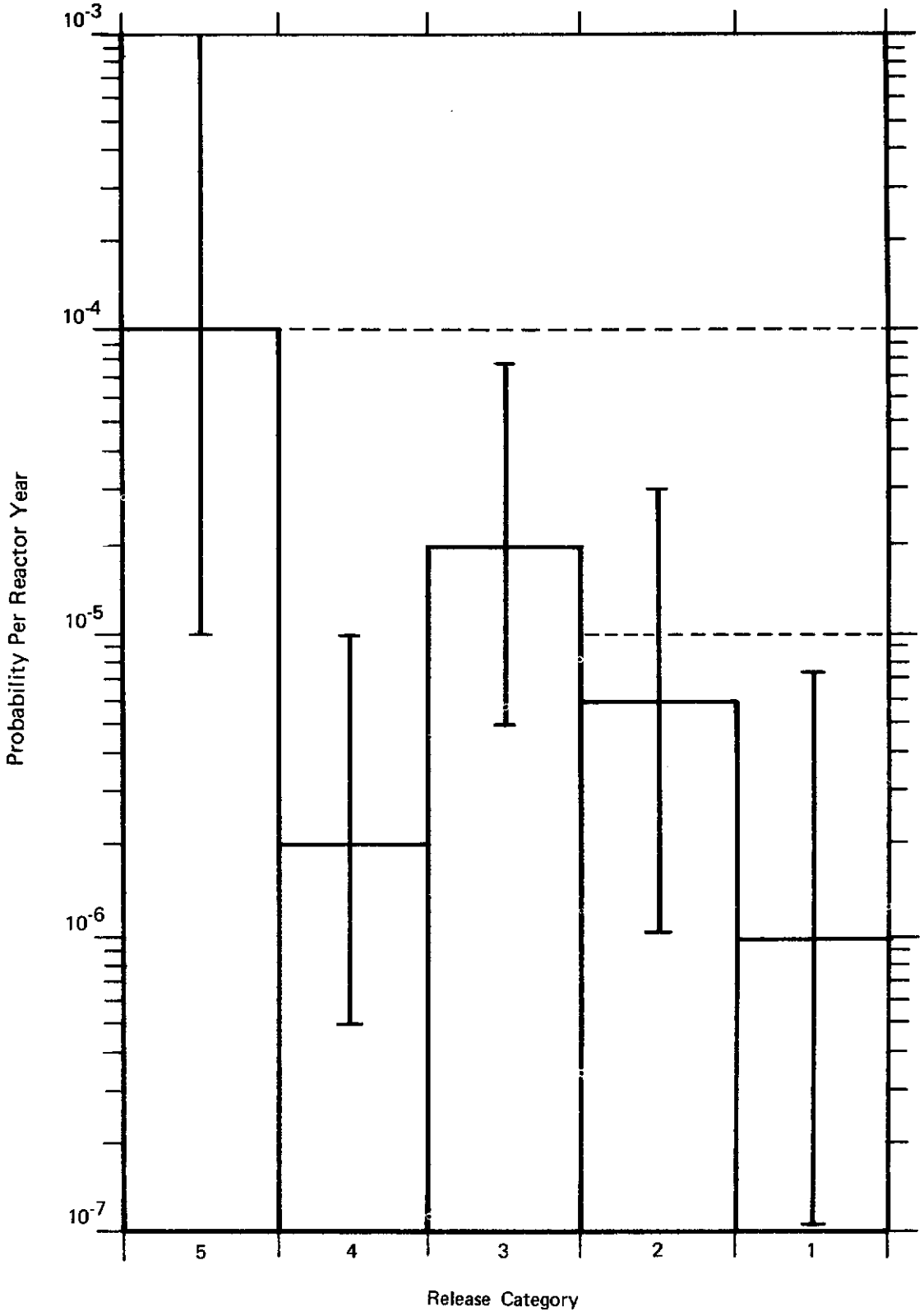


FIGURE 5-2 Histogram of BWR Radioactive Release Probabilities

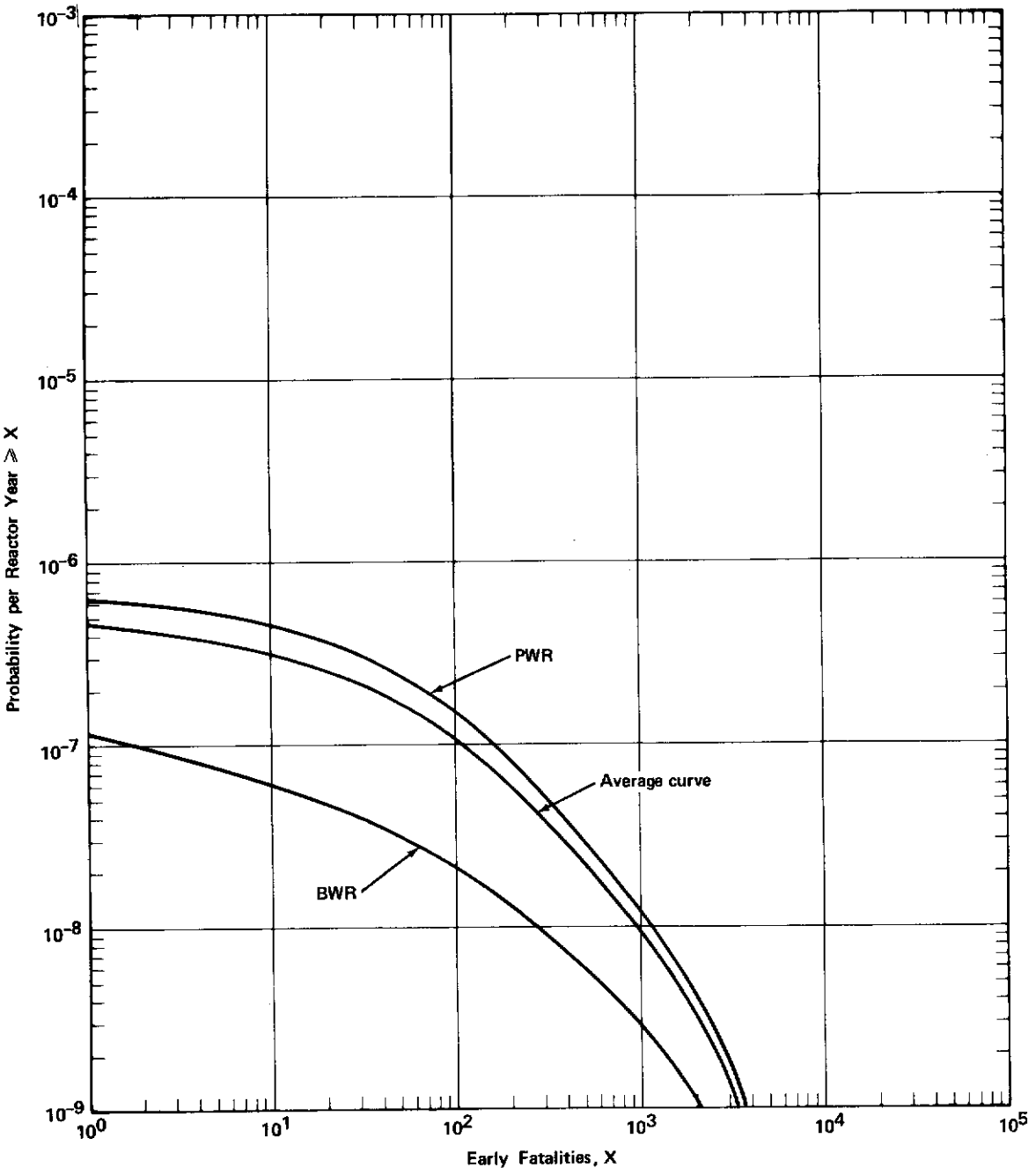


FIGURE 5-3 Probability Distribution for Early Fatalities per Reactor Year

Note: Approximate uncertainties are estimated to be represented by factors of 1/4 and 4 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

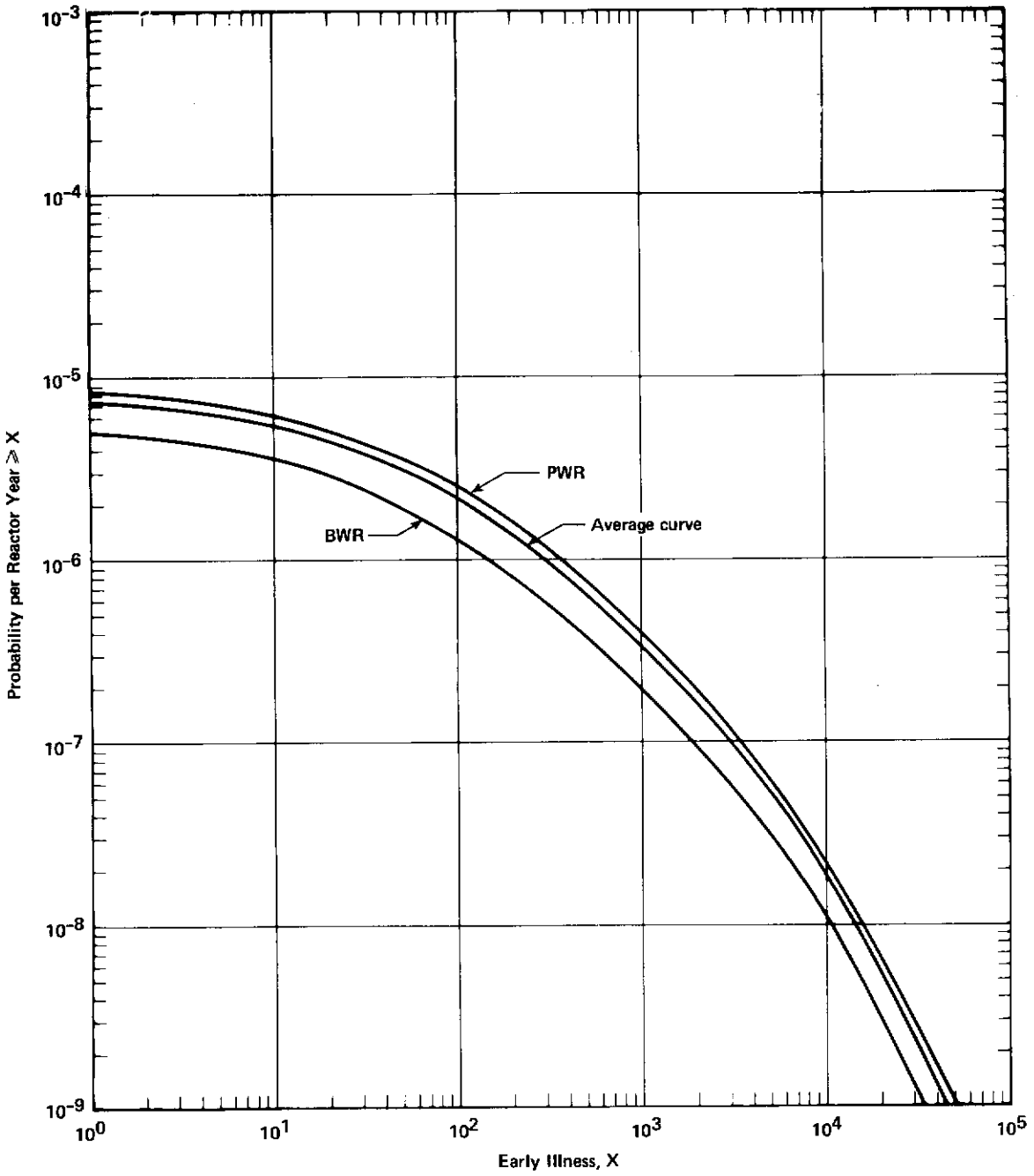


FIGURE 5-4 Probability Distribution for Early Illness per Reactor Year

Note: Approximate uncertainties are estimated to be represented by factors of 1/4 and 4 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

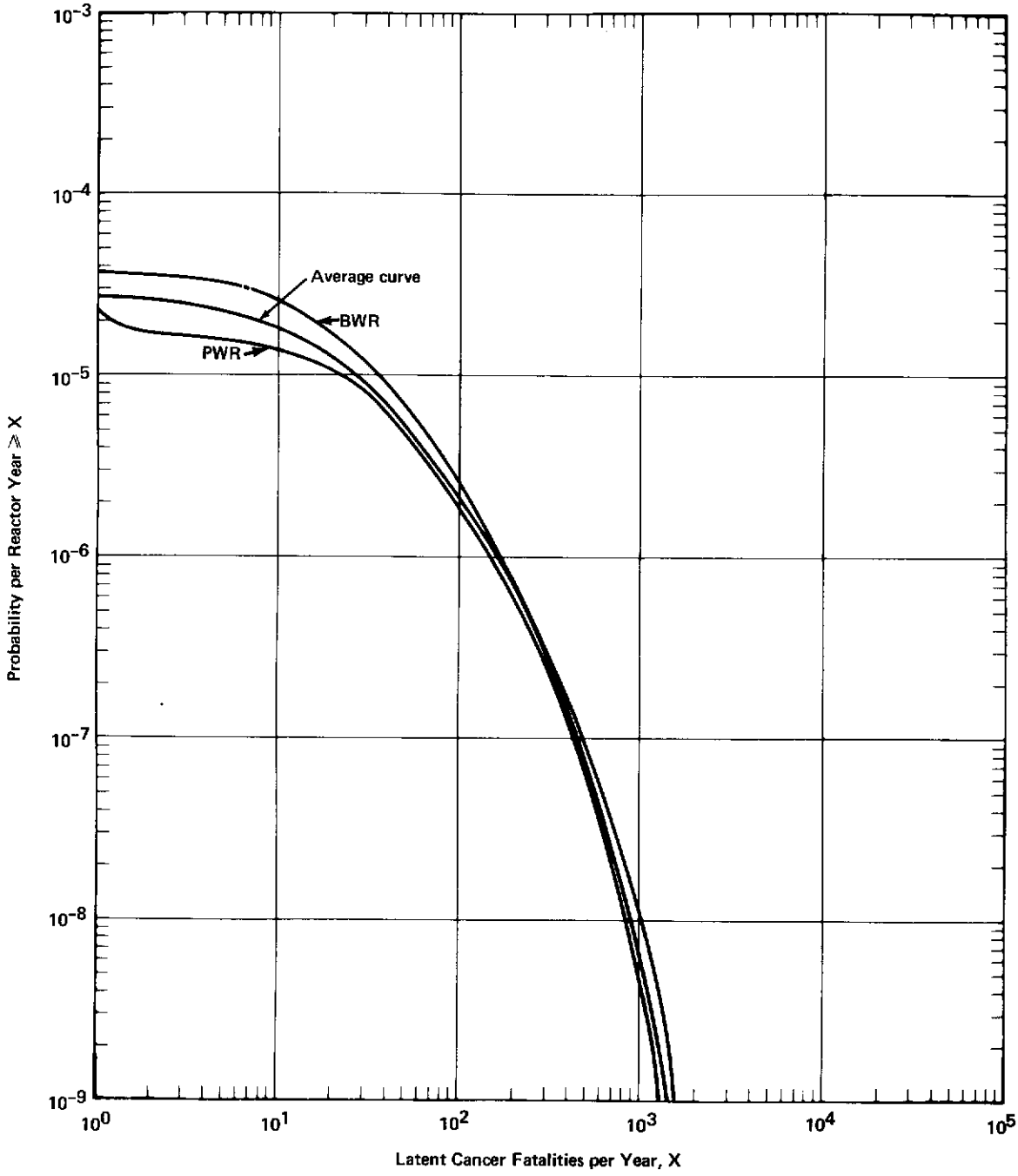


FIGURE 5-5 Probability Distribution for Latent Cancer Fatality Incidence per Reactor Year

Note: Approximate uncertainties are estimated to be represented by factors of 1/6 and 3 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

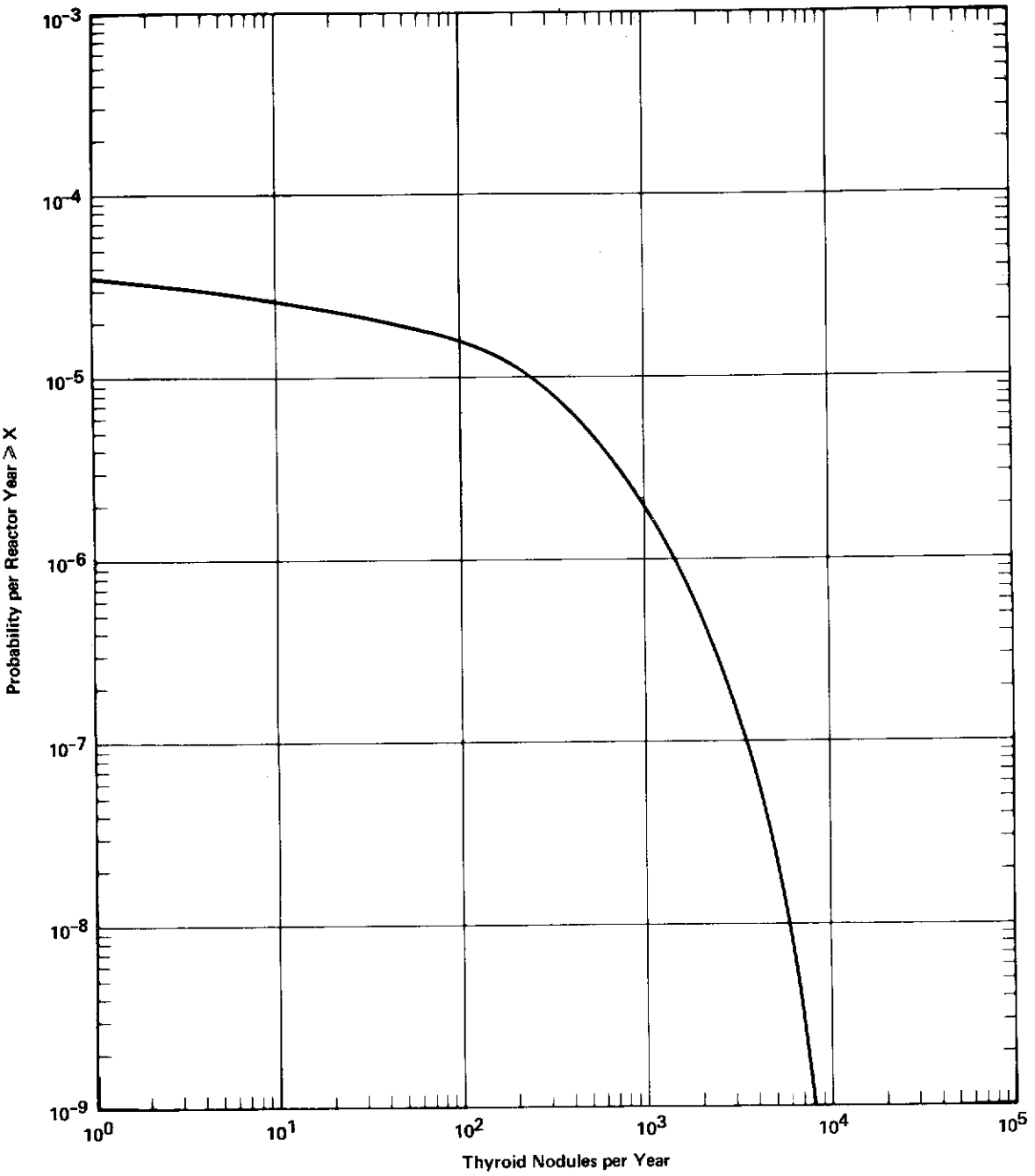


FIGURE 5-6 Probability Distribution for Thyroid Nodule Incidence per Reactor Year

Notes: 1. Approximate uncertainties are estimated to be represented by factors of 1/3 and 3 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

2. PWR and BWR are nearly identical.

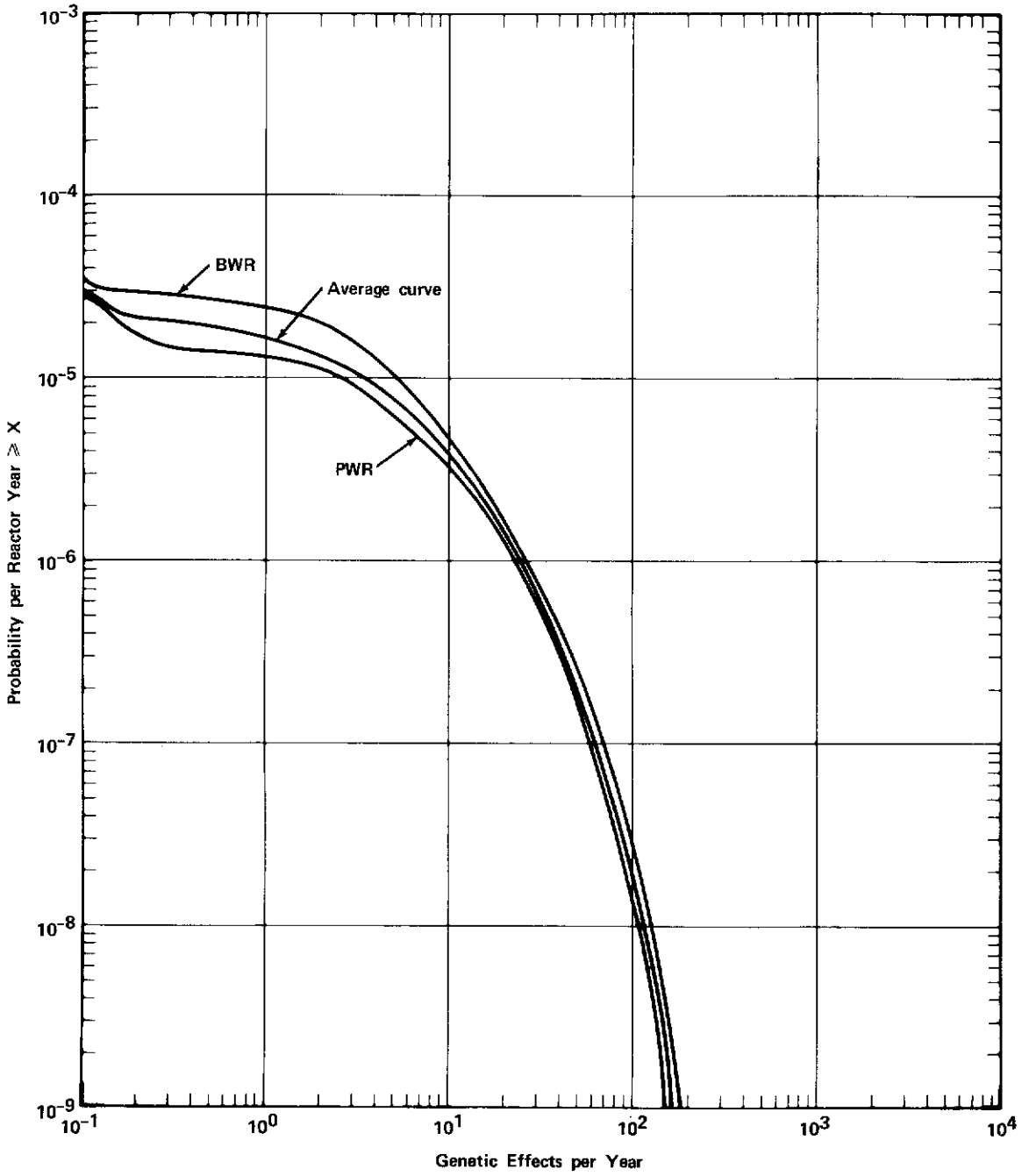


FIGURE 5-7 Probability Distribution for Incidence of Genetic Effects per Reactor Year

Note: Approximate uncertainties are estimated to be represented by factors of 1/3 and 6 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

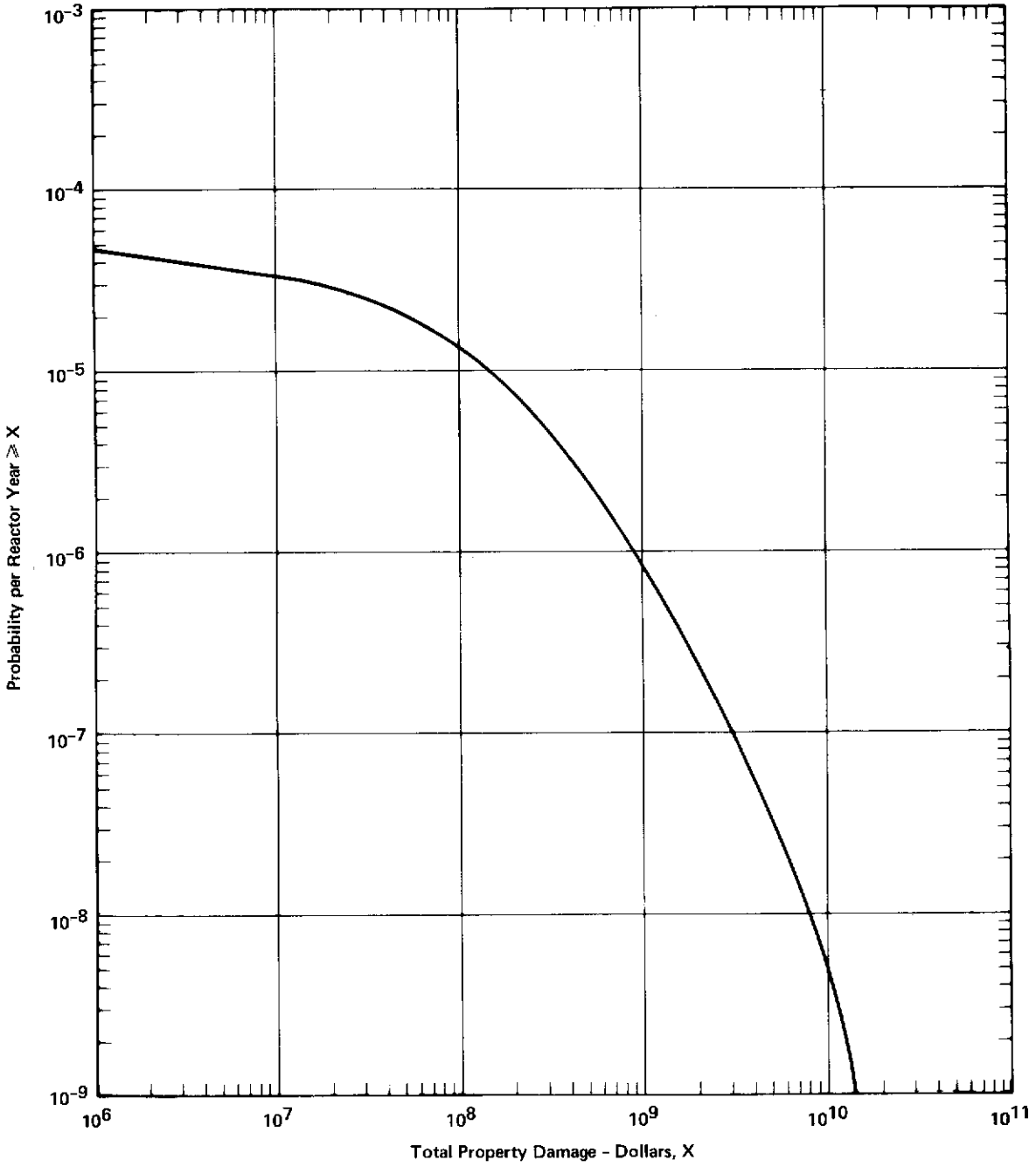


FIGURE 5-8 Probability Distribution for Property Damage per Reactor Year

Note: Approximate uncertainties are estimated to be represented by factors of 1/5 and 2 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

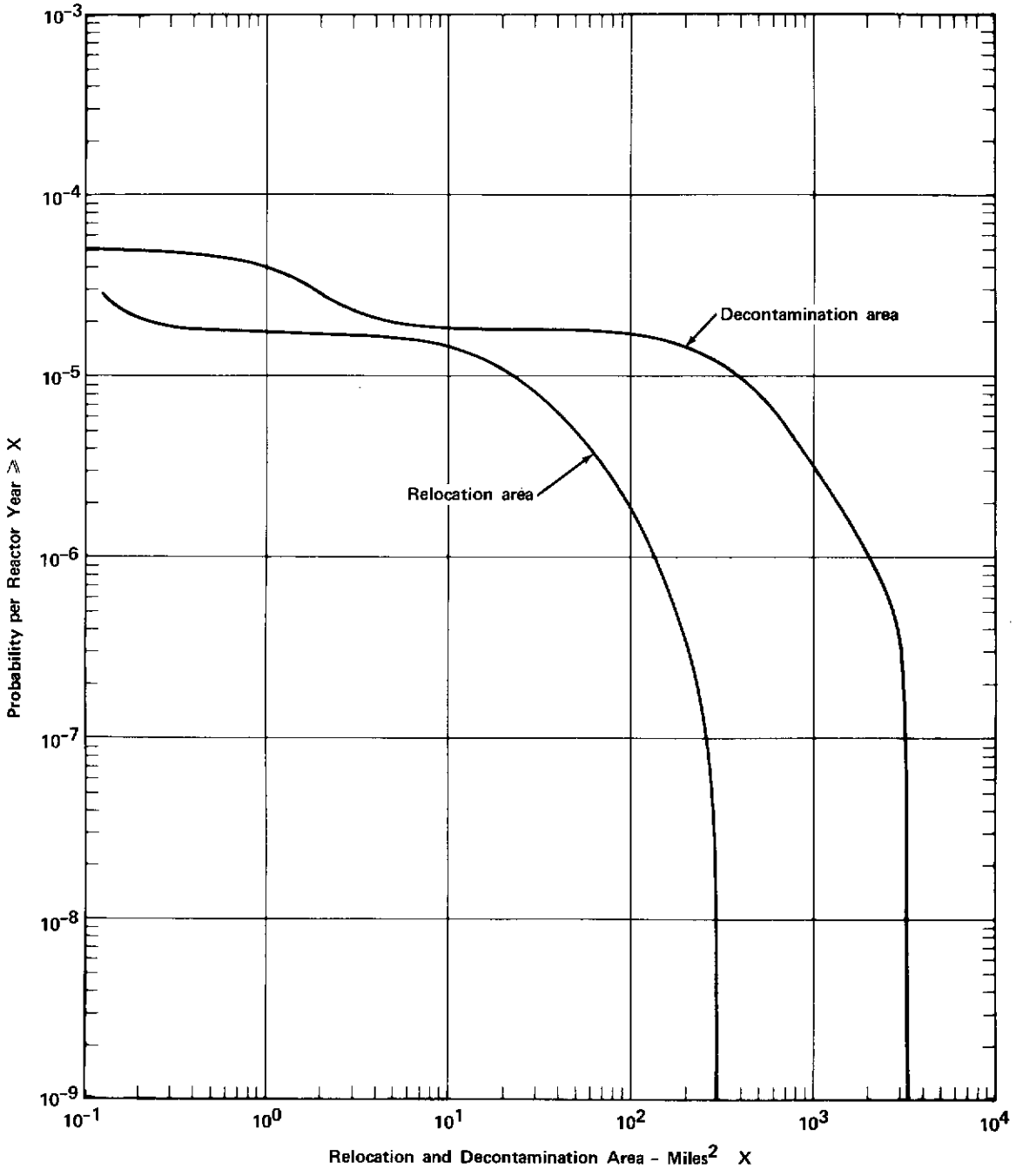


FIGURE 5-9 Probability Distribution for Relocation and Decontamination Area per Reactor Year

Note: Approximate uncertainties are estimated to be represented by factors of 1/5 and 2 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

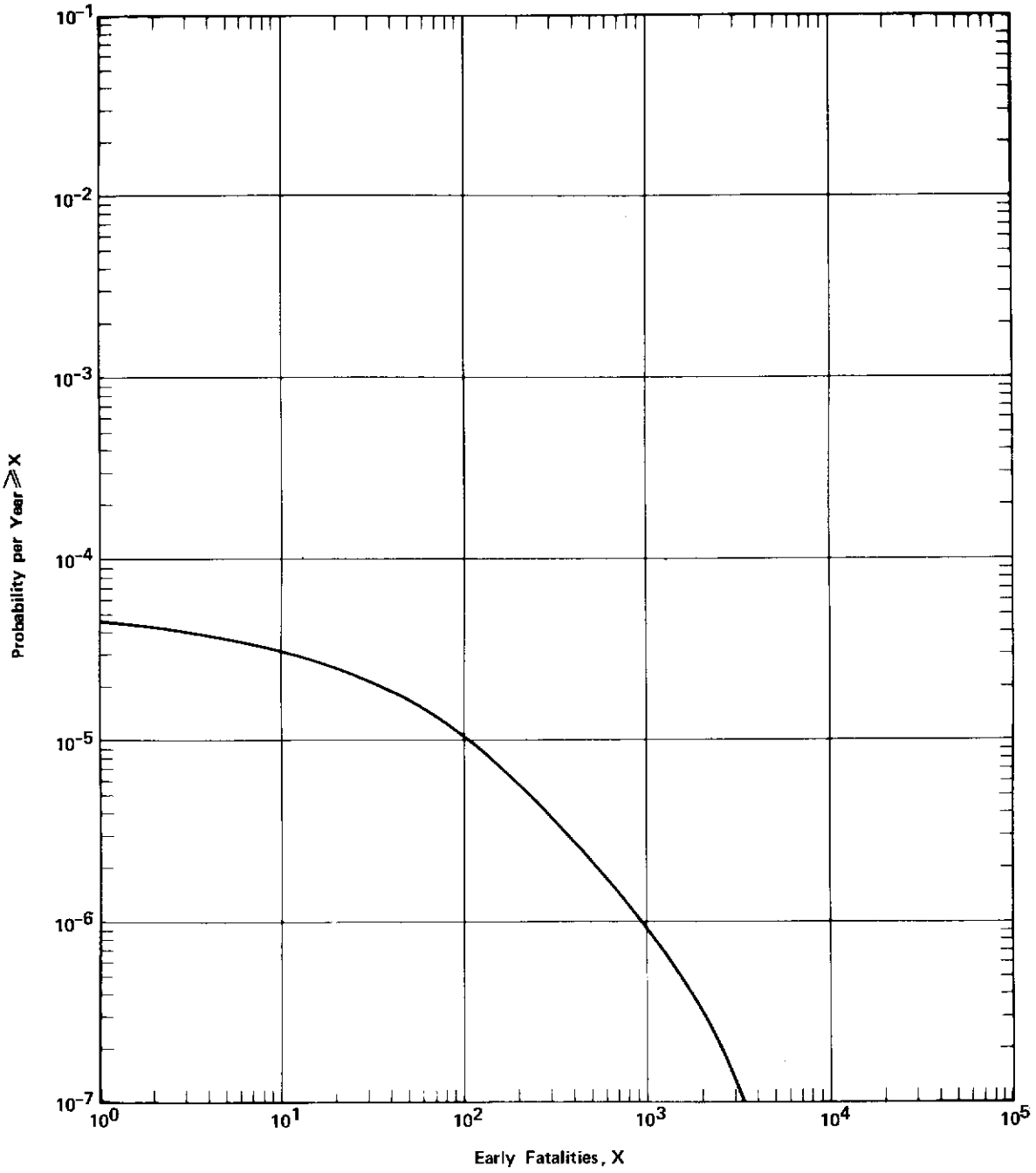


FIGURE 5-10 Probability Distribution for Early Fatalities per Year for 100 Reactors

Note: Approximate uncertainties are estimated to be represented by factors of 1/4 and 4 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

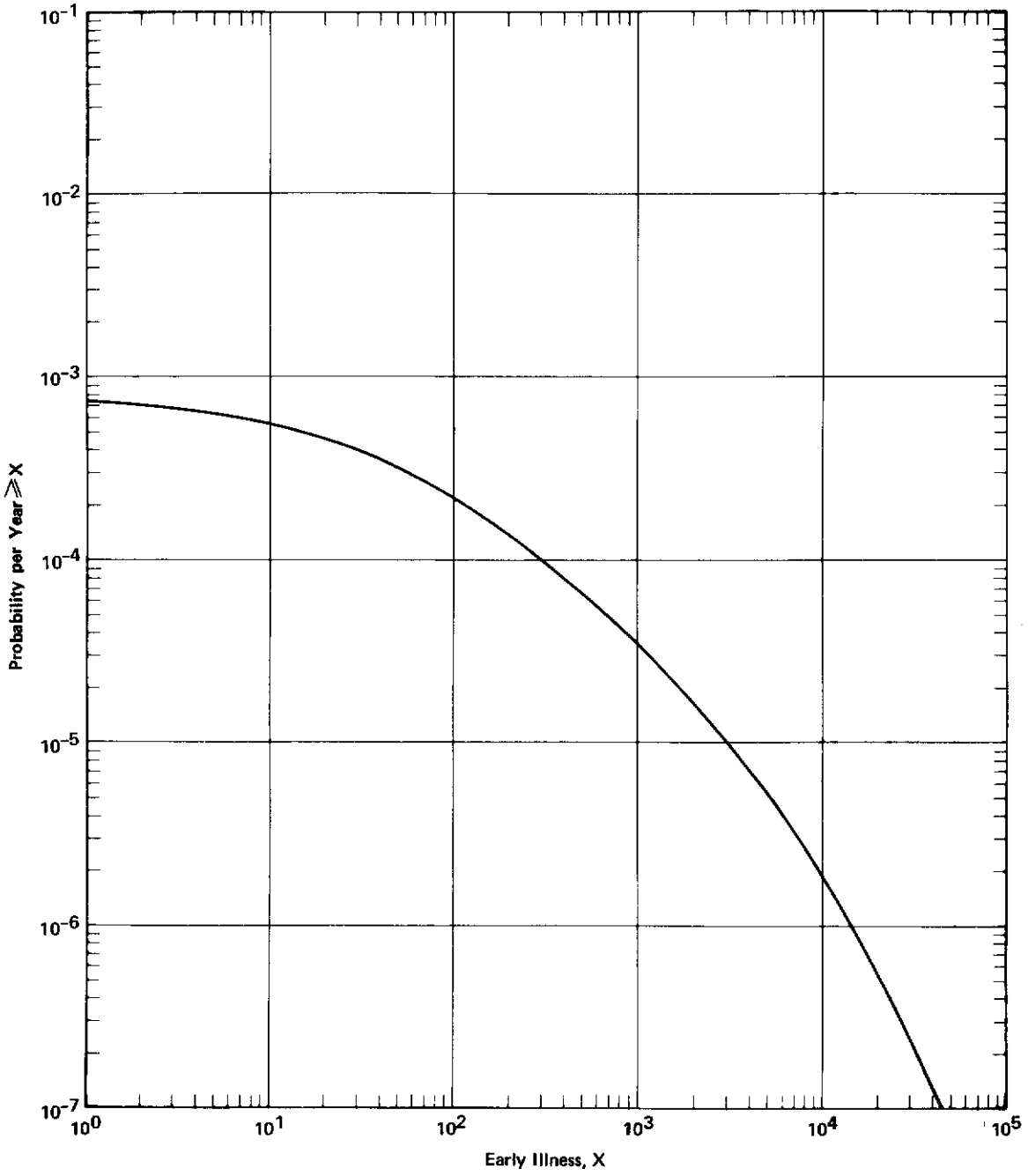


FIGURE 5-11 Probability Distribution for Early Illness per Year for 100 Reactors

Note: Approximate uncertainties are estimated to be represented by factors of 1/4 and 4 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

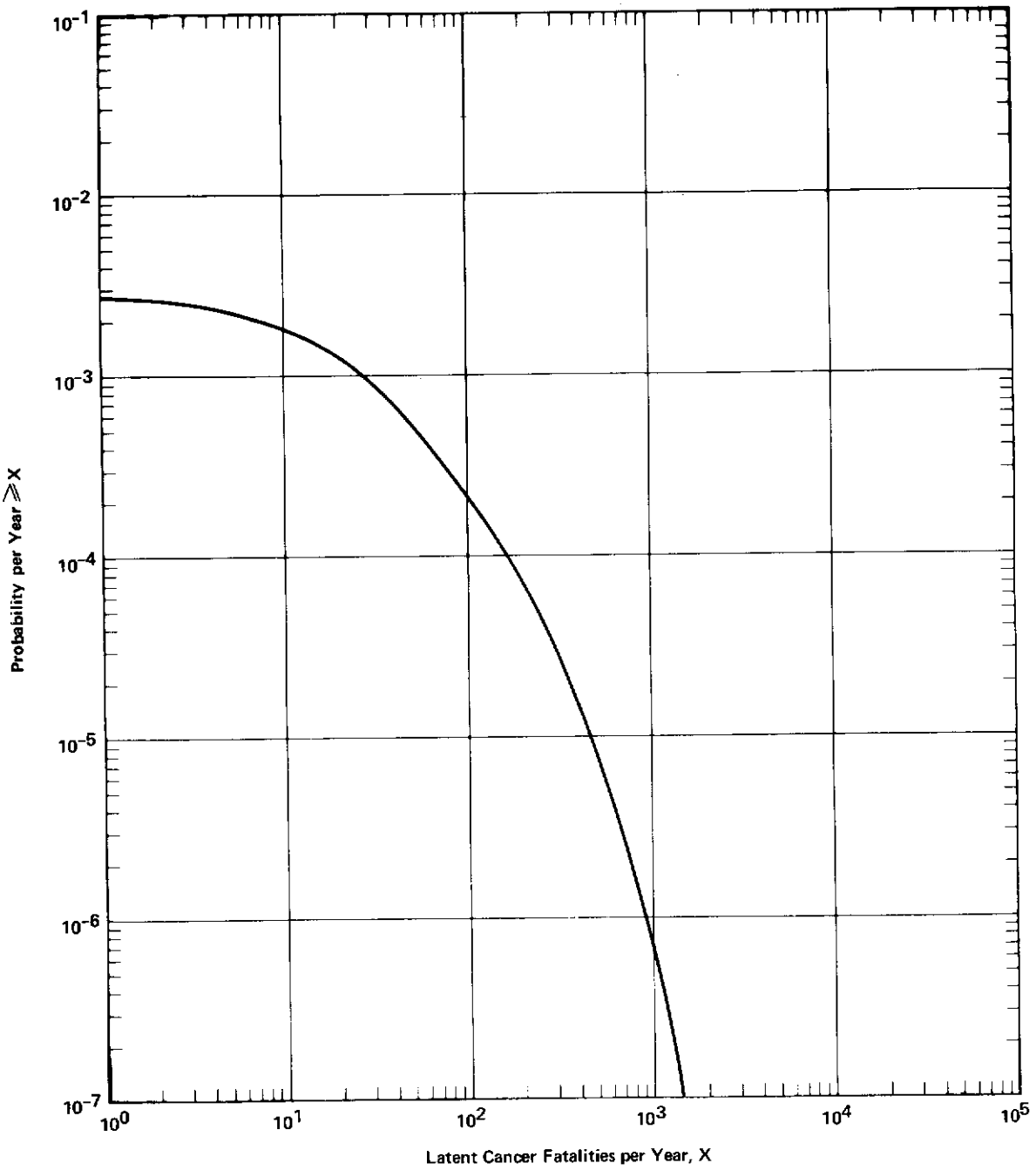


FIGURE 5-12 Probability Distribution for Latent Cancer Fatality Incidence per Year for 100 Reactors

Note: Approximate uncertainties are estimated to be represented by factors of 1/6 and 3 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

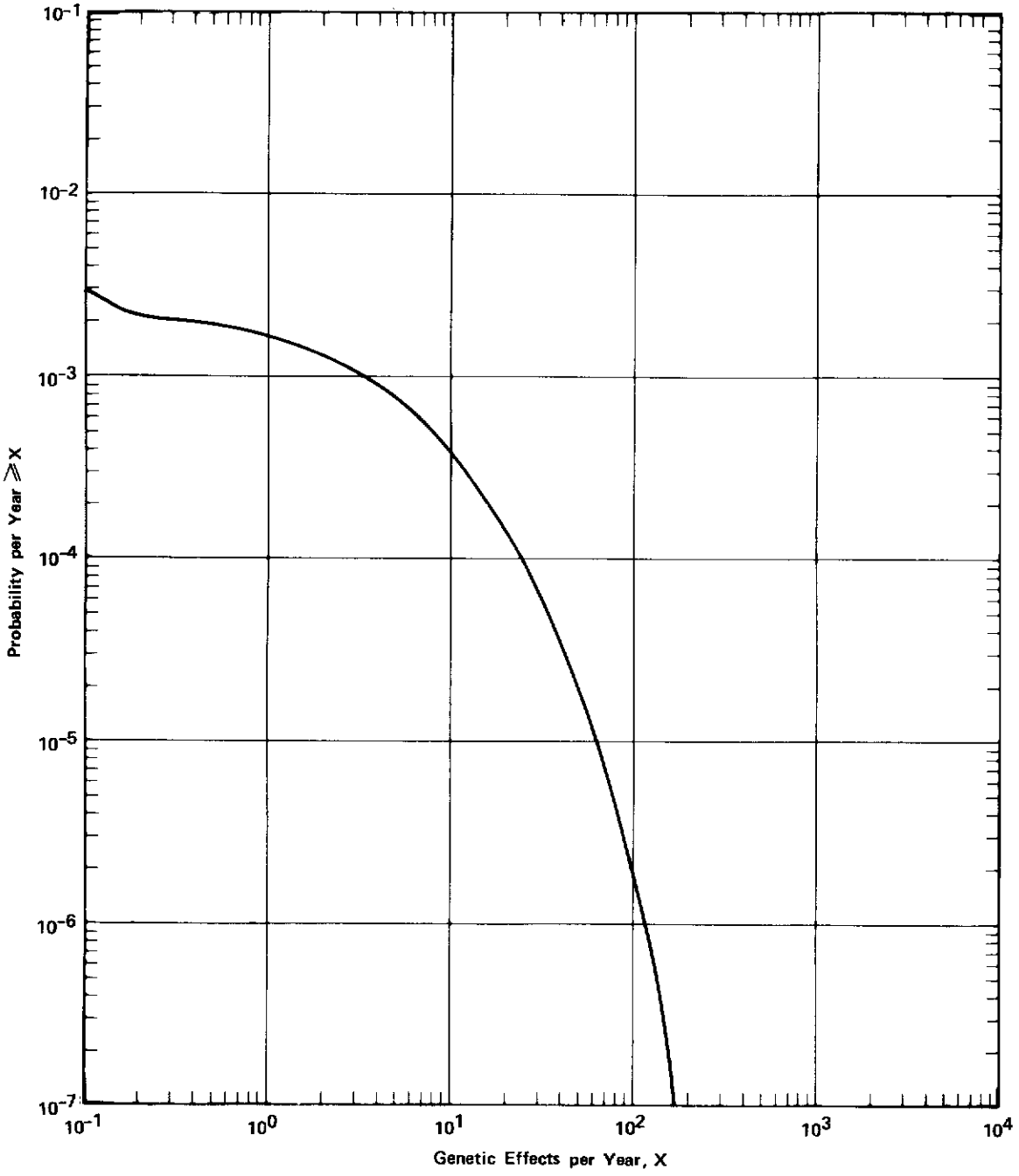


FIGURE 5-13 Probability Distribution for Incidence of Genetic Effects per Year for 100 Reactors

Note: Approximate uncertainties are estimated to be represented by factors of 1/3 and 6 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

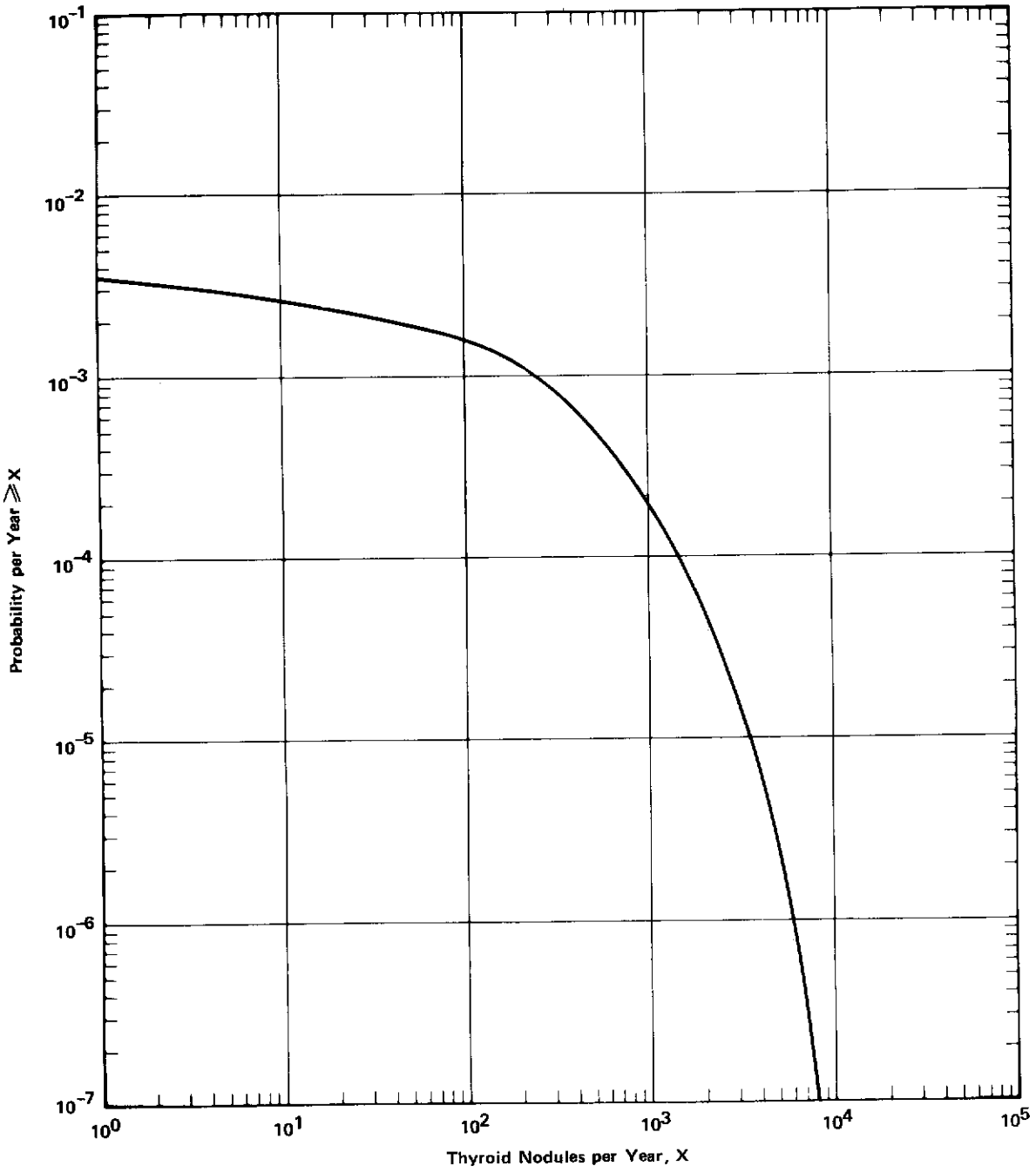


FIGURE 5-14 Probability Distribution for Thyroid Nodule Incidence per Year for 100 Reactors

Note: Approximate uncertainties are estimated to be represented by factors of 1/3 and 3 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

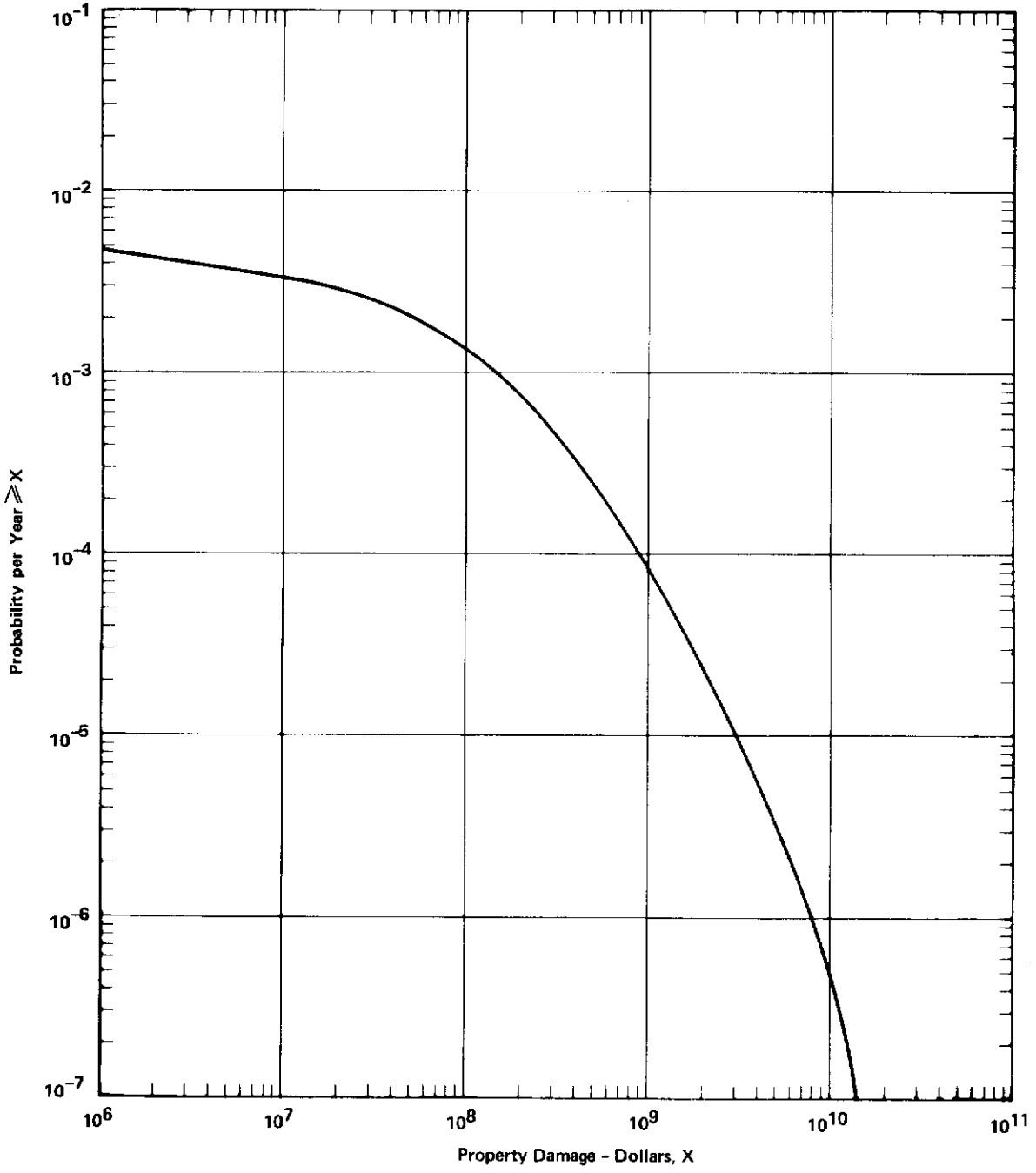


FIGURE 5-15 Probability Distribution for Property Damage per Year for 100 Reactors

Note: Approximate uncertainties are estimated to be represented by factors of 1/5 and 2 on consequence magnitudes and by factors of 1.5 and 5 on probabilities.

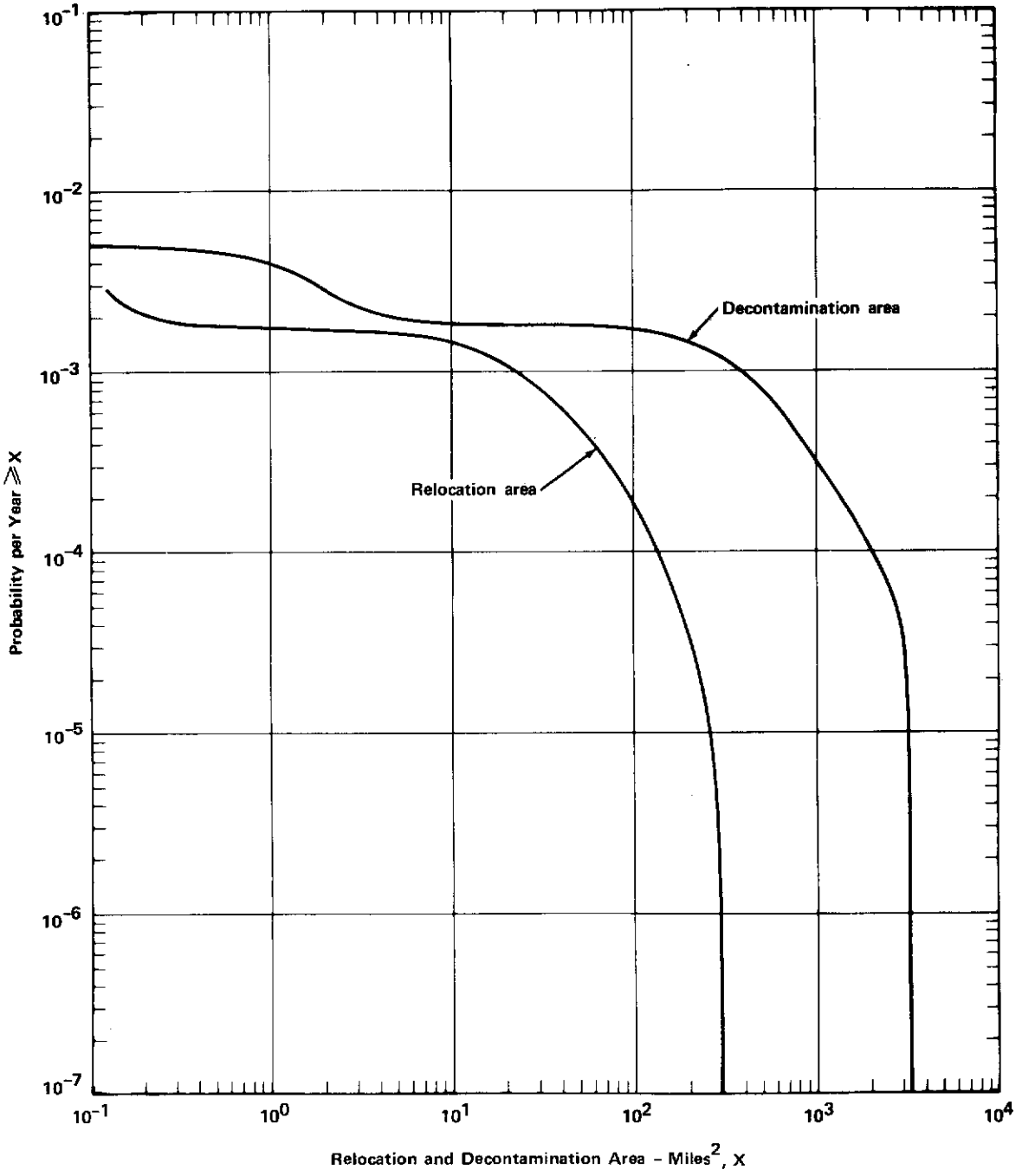


FIGURE 5-16 Probability Distribution for Relocation and Decontamination Area per Year for 100 Reactors

Note: Approximate uncertainties are estimated to be represented by factors of 1/5 and 2 on consequence magnitudes and by factors of 1.5 and 5 on probabilities.

Chapter 6

Comparison of Nuclear Accident Risks to Other Societal Risks

6.1 INTRODUCTION AND SUMMARY

The meaning of risk has been discussed in detail in Chapter 2, and it was noted that risk can be expressed in different ways, each of which is useful in understanding some aspects of the overall risk. In this chapter the potential risks associated with accidental radioactive releases from nuclear power plants that were predicted in Chapter 5 are compared to other risks to which society is exposed. Early fatalities, latent illnesses, and property damage are compared on the basis of risk to individuals as well as the overall societal risks.[1]

In the individual risk comparisons in section 6.2 and the societal risk comparisons in section 6.3, the risk from potential reactor accidents is shown as a combined average risk. It is obtained by multiplying the consequences associated with each of the release categories by its probability in order to express the risk as an average consequence per year. The summation of these gives the combined average risk from potential reactor accidents. In section 6.4, comparisons to risks from other large consequence events are made on the basis of consequence/frequency distributions. These provide perspective on the relative significance of the estimated consequence of reactor accidents, which have never occurred, compared to accidents which have actually occurred or can be estimated as a result of natural phenomena and other technological endeavors of man. Sections 6.2, 6.3, and 6.4 provide supporting information for the following summary of these risk comparisons.

In Table 6-1, the predicted individual and societal risks from nuclear power plant accidents are compared with the total risk from all other accidents.

Reactor accident consequences as functions of accident probabilities are compared with other low probability-high consequence events in Figs. 6-1, 6-2, and 6-3. Comparisons of fatalities in man-caused events and natural events are shown, respectively, in Figs. 6-1 and 6-2. A comparison of both man-caused and natural events is shown in Fig. 6-3. On all three figures, the curves for reactor accidents are based on 100 operating reactors.

It is apparent from Table 6-1 and Figs. 6-1, 6-2, and 6-3 that the total nuclear risk is small compared to the total risks from man-caused or natural events. Also, the figures indicate that earthquakes, hurricanes, dam failures, and chlorine accidents all have the potential for large consequence events at frequencies greater than reactors.

6.2 INDIVIDUAL RISK OF FATALITY AND INJURY

6.2.1 FATALITIES

Table 6-2 shows the death rates and risk of death per individual for three general categories: diseases, accidents, and other causes. Although these data from the 1973 Statistical Abstracts of the U.S. are for 1969, a review of other years shows the values change very little from year to year.

It is to be expected that certain population subgroups, classified by age, occupation, leisure activity, etc., will show significant deviation from these averages.

It is logical that risks from nuclear accidents should be compared to risks from other accidents and from natural phenomena in order to give added perspective to their meaning. In addition, since nuclear accidents can be expected to affect all groups within the exposed population, it is also useful to compare them to those groups that have the smallest risk of accidental fatality.

---

[1] Unless otherwise noted, the statistical information presented in the tables in this chapter for non-nuclear risks was obtained from the following sources:
(a) Statistical Abstracts of the United States 1973, U.S. Dept. of Commerce
(b) Accident Facts 1972, National Safety Council
(c) World Almanac, 1972

The statistics on accidental fatalities for the entire U.S. population are given in Table 6-3. Clearly many of these fatalities are associated with voluntary activities and it is to be expected that cautious individuals can substantially reduce their risk relative to that of the population average. Such potential risk reductions are indicated by the following two examples.

In recent years about 200 fatalities/year have occurred in commercial aircraft accidents. Of these, about 20 fatalities per year involved people on the ground who were killed by the falling aircraft. Thus, even the individual who does not fly cannot reduce his risk to zero because of this. His risk of death from this cause becomes about 10^{-7} per year (20 divided by the population of the U.S.).

In the case of automobile fatalities, the average individual risk is about 3×10^{-4} per year. Of the approximately 50,000 fatalities per year, about 20% are pedestrians (i.e., not occupants of the vehicle). By not riding in vehicles the individual's risk can, on the average, be reduced by about a factor of 5. Table 915 of the Statistical Abstracts of the U.S. for 1973 further indicates that about 500 motor vehicle fatalities occur each year to people who are neither auto occupants nor pedestrians on the roadway (i.e., crossing at intersections, walking along the highway etc.). Thus, even a person who never rides in a motor vehicle or enters a roadway can, on the average, reduce his individual risk from this cause by only a factor of about 100, or to about 3×10^{-6}. Clearly it is almost impossible to live in the U.S. and not ride in a motor vehicle or cross a street, so very few people would be able to achieve such a reduction in their risk of death in a motor vehicle accident.

A review of the large variety of accident risks that exists, as shown in Table 6-3, shows that although a careful person can probably take some action to reduce his risk to some types of accidents, he certainly cannot make his total accident risk zero. Thus, it seems reasonable to assume that even the most careful of individuals could not expect to reduce his risks from accidents by more than a factor of 100. Furthermore, to achieve this would require a significant departure from the typical U.S. life style. Thus, the risk of accidental death to a very safety conscious individual could not be made much smaller than about 6×10^{-6} per year (a factor of about 100 less than the individual risk, noted in Table 6-3 for all accidents).

The average early fatality rate predicted for potential nuclear accidents for a total of 100 operating nuclear plants in the U.S. (see Chapter 5) is 0.003 per year. The study has also shown that only persons within about 25 miles of a nuclear plant may suffer early effects. The total number of people living within 25 miles of the 68 reactor sites in the U.S. is approximately 15 million (see Appendix VI). (Note that some sites have more than one plant, so the 68 sites are consistent with 100 plants.) Thus, the estimated risk per individual from reactors in this exposed group is thus 0.003 divided by 15 million, yielding 2×10^{-10} early fatalities per person-year in the exposed population.

In Table 6-4, this risk is compared to the individual risk of death from accidents due to all other causes. Even if significant factors are allowed in the estimation of the nuclear risk, it is still small compared to other accident risks.

6.2.2 INJURIES

Most accidents produce a significantly larger number of injuries than fatalities. The number of acute illnesses resulting from reactor accidents has been determined in the consequence analyses described in section 4.3 and Appendix VI. In Table 6-5 the average risk of acute illness from nuclear accidents (for a total of 100 nuclear plants) is compared to the average risks of injury in motor vehicle accidents and in all non-nuclear accidents, as well as to an estimated average accident risk of a very risk averse person.

Table 6-5 indicates that an individual's risk of injury from nuclear accidents is small compared to the injury risk from other accidents, even for the highly risk averse person.

6.3 SOCIETAL RISK

6.3.1 FATALITIES AND INJURIES

The individual risks discussed in the previous section can be expressed in a way that shows their effects on society as a whole. Table 6-6 shows the number of fatalities and injuries expected in the total U.S. and also the numbers expected among the 15 million people who live within 25 miles of reactor sites. The numbers for reactor accidents are taken from Chapter 5 and include both acute and latent effects. The table

indicates that the risks associated with nuclear power plant accidents are small compared to the total societal risk from accidents.

6.3.2 ECONOMIC LOSSES

The economic losses to society from various accidents are considerable. They are dominated by automibile accidents and fires. Some readily available statistics are shown in Table 6-7.

Table 6-7 indicates that reactor accidents have a negligible impact on the total risk of economic loss from man's activities and from natural events.

6.4 RISK FROM LARGE CONSEQUENCE EVENTS

The previous section indicates that the risk to society and individuals from nuclear plant accidents is small compared to other more common risks that society and individuals accept. However, it it recognized that society may be reluctant to accept large consequence events at the same level of risk as small consequence events. (See Chapter 2.) The possibility of large consequence accidents is often raised by those questioning the wisdom of widespread use of nuclear power. Therefore, it is important to compare the probability/consequence distributions of nuclear accidents with those of other potential large consequence events.

In general, large consequence events can be divided into two types, natural events and man-made events (i.e., those directly involving man-made facilities, structures, etc.). Natural events which can cause large consequences include earthquakes, floods, hurricanes, tornadoes, and meteor impacts. Those classified as man-made events include: fires, explosions, airplane crashes, dam failures, release of toxic chemicals and release of radioactivity. These general categories distinguish between events over which man has little control and those for which he is primarily responsible. While treated independently in the following discussion, these two categories are not entirely independent since natural phenomena can cause serious accidents involving the man-made facilities and structures (e.g., an earthquake might cause a dam failure).

From a review of the historical record of the last 50 to 100 years it is possible to calculate, for many of the above events, the rate of occurrence of events with large consequences. Thus, information on some large consequence events with probabilities larger than 1 in about 100 can be obtained from actual experience. However, it is also possible to imagine sets of circumstances which could result in consequences much worse than those that have actually been observed. Generally, such events have probabilities so small that it would be unusual for them to have been observed in a period of 100 years. In many cases, the magnitude and probability of these events can be extrapolated from known data. In other cases, such as the nuclear plant accidents treated in this report, the probabilities and magnitudes must be estimated from an understanding of the nature of the phenomena. Both of these techniques were used in the analyses that support the following discussion.

The probability versus consequence curves in this section are based on observations of actual occurrences (plus some small extrapolation). Since they are statistical estimates based directly on data, standard confidence bounds can be calculated which show the incertainties in the curves. For a particular curve, the spread of the confidence bounds will increase as the consequences increase, showing the increasing uncertainty as consequences become larger.

Treating the observed phenomenon as a Poisson process, the 95% upper bound on the probability for a particular consequence is obtained by multiplying the best estimate probability by the factor $\chi^2_{.95,\,2r+2}/2r$, where r is the number of observations used in determining the probability value and $\chi^2_{.95,\,2r+2}$ is the 95th percentile of the tabulated chi square distribution with 2r+2 degrees of freedom. The 5% lower bound is obtained by dividing by the factor $2r/\chi^2_{.05,\,2r}$ where $\chi^2_{.05,\,2r}$ is the 5th percentile of the chi square with 2r degrees of freedom. These factors are obtained by standard, Poisson statistical treatments.[1]

The table below gives representative values of the confidence factors as a function of the number of observations r (for the probability versus consequence curves r is the number of observations with consequences greater than a particular value).

---

[1] See for example, N. L. Johnson and S. Kotz, Distributions in Statistics, Discrete Distribution, Houghton Mifflin Company, 1969, p. 96.

CONFIDENCE FACTORS

r	95% Upper Bound	5% Lower Bound
50	1.3	1.3
20	1.4	1.5
10	1.7	1.8
5	2.1	2.5
1	4.7	19.4

As seen from the table, the confidence factors ("error factors") dramatically increase for only one observation (r=1).

The smallest consequence values on the probability versus consequence curve will have the largest r values and hence will have relatively small confidence factors multiplying and dividing the estimated probability value. For the curves which are plotted, the value of r for the lowest consequences is roughly 50 thereby giving confidence factors of 1.3 (i.e., there is approximately 30% error on the corresponding probability estimates).

The largest consequence point on a curve will have the value r=1, independent of the particular curve, since one observation gives the peak consequence value. From the table the upper bound factor is thus approximately 5 and the lower bound factor approximately 20. While the plotted curves show only the values calculated from the data, the preceding factors can be applied to any of the curves to obtain the probability spread at the maximum consequence value.

6.4.1 HURRICANES

The U.S. Department of Commerce has recently issued a report entitled "Some Devastating Hurricanes of the 20th Century." Table 6-8 summarizes some pertinent data from that report. The points shown in Fig. 6-4 are based on an analysis of these data. A log-log plot has been used to accommodate the large changes in the variables.

The manner in which the data in the tables in this section of the report are used to generate data points for the corresponding figures is indicated by the following example for Table 6-8 and Fig. 6-4. For convenience the individual data items in Table 6-8 are listed and numbered according to the number of fatalities. There are five hurricanes of more than 400 fatalities. Since the experience record is 73 years (1900-1972), the frequency is 5/73 = 0.068. Thus, Fig. 6-4 has a data point at 400 fatalities and a probability of about 7×10^{-2}. Similarly, Table 6-8 shows that during the 73 years period there were 32 hurricanes with 11 or more fatalities. Thus, Fig. 6-4 has a data point at 11 fatalities and a probability of 32/73 = 0.44. The other data points in Fig. 6-4 as well as those in other figures in this section were similarly calculated.

The largest observed event in U.S. history was the 6000 fatalities in the Galveston Hurricane of 1900. Based on one occurrence in 73 years, such an event has a probability of about 0.013. A roughly estimated error band for the fatality curve in Fig. 6-4 should lie mostly below such a point since it is reasonable to expect that with today's understanding of hurricanes and the communication systems available in the U.S. an event of such consequences will be considerably less likely than it was in 1900. For similar reasons there may be a temptation to say that such an event could not occur today; however, such a hurricane did occur only six years ago, with over 300 fatalities.

It seems clear that a hurricane more severe than any yet recorded, particularly one affecting the ever increasing population density in the eastern U.S., could produce very large numbers of fatalities. Thus, although the extrapolation in Fig. 6-4 cannot be claimed to have high precision, it appears to be a reasonable estimate.

As might be expected, because of the increased amount and value of property exposed, the property damage per hurricane has been increasing dramatically in recent years. The curve (see Fig. 6-4 showing property damage has, therefore, been based on only the last 21 years (1952-1972). The extrapolation of this curve indicates that hurricanes like Agnes ($3.5 billion damage) might be expected with a probability of 0.01-0.05 or a return period of every 20 to 100 years. During the last 20 years there have been four hurricanes with damages in the 1 billion dollar range and an average of one hurricane per year with damage exceeding 10 million dollars.

6.4.2 TORNADOES

The statistics on tornadoes have been summarized by the Department of Commerce in a recent bulletin (Ref. 1). In addition, major tornadoes from 1925 to 1971, inclusive, are listed in the 1973 World

Almanac. Based on these records, Fig. 6-5 provides a plot of tornado frequency versus fatalities. The total number of tornado-related fatalities during the 1953-1971 period is 2124, or an average of 118 per year. The largest event in the 1925-1971 period caused 689 fatalities in Indiana on March 18, 1925. Even though a tornado warning system was in effect, 271 were killed by tornadoes on April 11, 1965. Thus, although such a system is useful, it evidently cannot prevent large consquence events.

The property damage from tornadoes has exceeded 50 million dollars per year during the period 1965-1971. Detailed data on damage per event have not been found, but because of their localized nature the dollars of damage per tornado is expected to be at least a factor of 10 less than for hurricanes. For this reason tornado damage has not been estimated.

6.4.3 EARTHQUAKES

The major earthquakes in the U.S. since 1900 and their consequences are listed in Table 6-9. These data have been used to obtain the points on the curves in Fig. 6-6. A recent NOAA study (Ref. 2) has estimated that a recurrence of the San Francisco earthquake today would result in 1 billion dollars damage to single family dwellings and presumably about an equal amount to other structures. Therefore, the damage curve of Fig. 6-6 has been adjusted to reflect this estimate. A similar upward adjustment has also been made in the fatality curve to account for probable increased fatalities. The extrapolation of the curves, beyond the points based on prior earthquakes, is aided by the NOAA study that estimated the consequences of a large earthquake in the city of Los Angeles. This study estimated the probable fatalities and property damage from an earthquake with a return period of about 100 years. The fatalities were estimated to be between 10,000 and 20,000. The property damage to single family dwellings was estimated to be between 1.5 and 2.5 billion dollars. In the United States single family dwellings represent about 40% of the value of all dwellings and therefore the total property damage could easily be a factor of 2 larger.

Thus, for a frequency of about 0.01 per year (i.e., 1 in 100 years) the NOAA report estimates fatalities of 10,000 to 20,000 and property damage of 3 to 5 billion dollars. (The estimates become substantially larger if the potential failure of certain dams in the Los Angeles area is taken into account.) These two estimated points are shown by squares on Fig. 6-6. Since the earthquake frequency is substantially higher in California than elsewhere in the U.S. these points are assumed to represent such earthquakes for the entire U.S. The fact that these values of damage are so much higher than historical data reflects the fact that both the population density and property values have greatly increased in California in recent years. This is evident from the fact that the San Fernando earthquake had a relatively modest magnitude of 6.6 (Richter scale) and did 480 million dollars damage to structures, while the 1906 San Francisco earthquake, of magnitude 8.3, did only about 80 million dollars damage to structures, the balance being done by a subsequent fire. It seems reasonable to believe that the data points indicate consequences that are low compared to the probable consequences of similar earthquakes occurring today.

Since the data are relatively sparse the curves shown in Fig. 6-6 must be considered to have sizable error. However, a review of earthquakes that have occurred around the world shows fatalities as high as 143,000 in Tokyo in 1923 and nine others with fatalities greater than 10,000. Such potential consequences cannot be directly applied to the U.S. because of major differences in building codes and other factors. Nevertheless, an earthquake with very large consequences could also occur in the U.S. For example, the recent San Fernando earthquake almost failed the Van Norman Dam. Such a failure probably could have resulted in about 70,000 or more fatalities.

Based both on worldwide experience and estimates such as described above, extrapolation indicates that up to 10^5 fatalities might occur for a severe earthquake occurring in the U.S.

6.4.4 METEORITES

Major meteorite impacts onto the earth are known to have occurred in Arizona and Siberia. Should such an impact occur on a highly populated site very sizable loss of life and property damage would be expected. Blake (Ref. 3) has estimated the probability of such impacts and the expected loss of life. His predictions are for the entire world. The fatality curve in Fig. 6-7 shows Blake's results but with the probabilities reduced by a factor of 16 to reflect the fact that the U.S. contains 6% of the earth's land area.

The property damage from such events was not estimated by Blake. The damage curve in Fig. 6-7 assumes the same ratio of damage to fatalities as for earthquakes.

6.4.5 AIRPLANE CRASHES

In the 1960 to 1973 period there have been 67 major airplane crashes throughout the world. The number of crashes for several specific ranges of numbers of fatalities are summarized in Table 6-10.

Sixteen of the airplane crashes summarized in Table 6-10 occurred in the U.S. Analysis of the data for the U.S. gives the number of crashes/year with fatalities greater than 50 as 1.2 per year, greater than 100 as 0.47 per year, and greater than 150 as 0.11 per year. These results are plotted in Fig. 6-8. These fatalities were almost all occupants of the aircraft, and so the curve would appear to have a cutoff at a maximum of about 350, about the capacity of the largest planes. However, this limit does not apply to non-occupant fatalities that could occur in the event of an airplane crash. In four of the noted crashes five or more fatalities involved people on the ground. One crash included 71 such fatalities. Okrent (Ref. 4) has recently estimated the probabilities and fatalities associated with potential aircraft crashes into large gatherings or people, such as occur at football stadia, racetracks, etc. Figure 6-8 includes a point, representative of Okrent's estimates which provides the basis for the curve extending to high consequences at relatively low probabilities. Since there are numerous theaters, shopping centers and stadia throughout the country this extrapolation seems reasonable.

6.4.6 EXPLOSIONS

During the 1925-1971 period, 44 major explosions occurred throughout the world. The acute fatalities associated with these events were distributed as shown in Table 6-11. Twenty-two of the explosions represented in Table 6-11 occurred in the U.S. Thus, although the worldwide data have been used to obtain the shape of the curve in Fig. 6-9, the values in Table 6-11 and the curve has been shifted downward by a factor of 2 in probability since only half of the explosions occurred in the U.S. The extrapolation to high acute fatalities seems reasonable since rather large quantities of potentially explosive materials are shipped and stored throughout the U.S.

6.4.7 DAM FAILURES

There have been a number of dam failures in the world in the last 100 years. The major dam failures that occurred in the U.S. over the last 85 years are listed in Table 6-12.

In the U.S. there are over a hundred major dams whose failure rate has been estimated to be about 10^{-4} per dam per year (Ref. 5). Recent estimates (Ref. 6) indicate that at least 20% of these dams have substantial populations exposed below them, and that fatalities in the range of 1000 to 100,000 could occur in the event of failure of one of these dams. If there is a 50% chance that failure of one of these dams would result in 10,000 fatalities, then the probability of a dam failure that results in 10,000 fatalities is given by the following equation:

$$(20 \text{ dams}) \times \left(10^{-4} \frac{\text{failure}}{\text{dam-year}}\right) \times (0.5) = 1 \times 10^{-3}/\text{year}$$

As shown in Fig. 6-10 this agrees quite well with the extrapolation of the data.

6.4.8 FIRES

Considering only fires that have occurred in the U.S. since 1900, the largest number of fatalities, 602, occurred in the famous 1903 Iroquois Theater fire in Chicago. However, 491 fatalities occurred in the Coconut Grove fire in Boston in 1942.

The fatality data points plotted in Fig. 6-11 are based on these data and that from other fires that occurred in the U.S. since 1900.

In terms of property damage, the two largest fires have been the 1871 Chicago fire with losses of about $200,000,000, and the 1906 San Francisco fire that produced several hundred million dollars damage. Since the latter occurred as a result of an earthquake, its damage has been included in the previous estimates of earthquake consequences. The National Fire Protection Association lists the major U.S. fires each year in its publication, Fire Journal. The results of an analysis of the major fires from 1964 through 1972 are given in Table 6-13. These data are plotted in Fig. 6-11.

The largest fires included in the analysis were an industrial fire at 75 million dollars damage and three large

forest fires, each of which burned over 40,000 acres. The value of the loss in the forest fires is based on an estimate of 40,000 acres. The value of the loss in the forest fires is based on an estimate of $1000/acre for timber loss and damage to the watershed. Thus, these three fires were considered to be in the 40 to 50 million dollar loss category.

6.4.9 HAZARDOUS CHEMICAL RELEASES

In the U.S. there have been a number of accidents involving releases of hazardous chemicals. The predominant releases occur during transport and the major commercial chemicals involved are chlorine, ammonia, ethylene oxide, and hydrogen fluoride. Because of the relatively large amounts shipped and its inherent toxicity, chlorine has been selected as a basis for assessing the public risk associated with major accidents involving hazardous chemicals.

A recent study (Ref. 7) indicates that transport by railroad tank car poses the most serious public risk associated with chlorine. This occurs because of the accident frequency, the large amount of chlorine shipped by this mode (70 percent of all shipments) and the proximity of rail routes to densely populated areas. The frequency of accidents involving the release of all or a substantial fraction of a tank car's cargo is at least once every ten years. While prior accidents of this type have resulted in only one fatality in 50 years, there is obviously a potential for accidents causing large numbers of fatalities. The referenced study (Ref. 7) investigated the potential frequency and consequnces of such accidents. The study noted that nearly all U.S. railroad shipments of chlorine are made in the eastern states. The probability of a given population density at an accident site was based on the assumption that accidents are uniformly probable along the rail routes used. Population density along these routes was approximated by the density distribution for the state of Ohio. The average frequency of the occurrence of several combinations of wind speed and atmospheric stability in the Eastern U.S. was used to determine the area exposed to a lethal dose of chlorine vapor. The potential net risk was calculated for an accident involving the rupture of a tank car and the release of 90 tons of liquid chlorine.

The results of the chlorine accident study are shown in Fig. 6-12, which shows the estimated accident frequency versus fatalities for chlorine releases with and without popluation evacuation. The evacuation model used is based upon one developed by the Environmental Protection Agency (Ref. 8). The curves indicate that only in the relatively high consequence events are the predicted fatalities reduced significantly by accounting for the effects of evacuation. This is evidently due to the delay time incorporated in the particular evacuation model used in the analyses.

References

1. "Severe Local Storm Warning Service and Tornado Statistics 1953-1971," U.S. Department of Commerce.

2. "A Study of Earthquake Losses in the Los Angeles, California Area," prepared by NOAA for the Federal Disaster Assistance Administration.

3. Blake, V. E. "A Prediction of the Hazards from the Random Impact of Meteorites in the Earth's Surface," Sandia Labs, Aerospace Nuclear Safety, December 1968, SC-RR-68-388.

4. D. Okrent et al., "Airplane Crash Risk to Ground Population," UCLA-ENG-7424, March 1974.

5. P. F. Gast (ANL), "Divergent Public Attitudes Toward Nuclear and Hydro-electric Plant Safety," Presented 6/73 at ANS Meeting, Chicago, Illinois.

6. D. Okrent et al., "Estimates of Risks Associated with Dam Failure," UCLA-ENG-7423, March 1974.

7. J. A. Simmons et al., "The Risk of Catastrophic Spills of Toxic Chemicals,' UCLA-ENG-7425, May 1974.

8. J. M. Hans, Jr. & T. C. Sell, "Evacuation Risks - An Evaluation," EPA-520/6-74-002, June 1974.

TABLE 6-1 RISK OF EARLY FATALITIES FROM NUCLEAR AND NON-NUCLEAR ACCIDENTS

Societal Risk		Individual Risk	
Early Fatalities per year in U.S.		Early Fatality Probability/Year	
Non-Nuclear[(a)]	Nuclear[(b)]	Non-Nuclear[(a)]	Nuclear[(b,c)]
115,000	4×10^{-2}	6×10^{-4}	2×10^{-10}

(a) Includes all non-nuclear accidents.

(b) Based on estimated values for 100 nuclear power plants. The values indicated are based on early lethalities only to make them comparable to other values listed.

(c) Based on the approximately 15 million people located within 25 miles of nuclear power plants. If the entire U.S. population of 200 million people were to be used, then the value would be 2×10^{-11}.

TABLE 6-2 U.S. FATALITIES - BY MAJOR CATEGORIES (1969)

Type	Fatalities/100,000 persons	Approximate Individual Risk Fatality Probability/year
Diseases	819	8×10^{-3}
Accidents	57.6	6×10^{-4}
Other Causes	76.2	8×10^{-4}
Total	951.9	1×10^{-2}

TABLE 6-3 INDIVIDUAL RISK OF EARLY FATALITY BY VARIOUS CAUSES

(U.S. Population Average 1969)

Accident Type	Total Number for 1969	Approximate Individual Risk Early Fatality Probability/yr[a]
Motor Vehicle	55,791	3×10^{-4}
Falls	17,827	9×10^{-5}
Fires and Hot Substance	7,451	4×10^{-5}
Drowning	6,181	3×10^{-5}
Poison	4,516	2×10^{-5}
Firearms	2,309	1×10^{-5}
Machinery (1968)	2,054	1×10^{-5}
Water Transport	1,743	9×10^{-6}
Air Travel	1,778	9×10^{-6}
Falling Objects	1,271	6×10^{-6}
Electrocution	1,148	6×10^{-6}
Railway	884	4×10^{-6}
Lightning	160	5×10^{-7}
Tornadoes	118[b]	4×10^{-7}
Hurricanes	90[c]	4×10^{-7}
All Others	8,695	4×10^{-5}
All Accidents (from Table 6-1)	115,000	6×10^{-4}
Nuclear Accidents (100 reactors)	—	2×10^{-10}[d]

(a) Based on total U.S. population, except as noted.
(b) (1953-1971 avg.)
(c) (1901-1972 avg.)
(d) Based on a population at risk of 15×10^6.

TABLE 6-4 INDIVIDUAL RISK OF EARLY FATALITY FROM NUCLEAR AND NON-NUCLEAR ACCIDENTS

Group Exposed	Individual Risk Fatality Probability/Year	
	Non-Nuclear	Nuclear[(a)]
U.S. Average	6×10^{-4}	2×10^{-10}
Very risk-averse person	6×10^{-6}	2×10^{-10}

(a) This risk is only applicable for 100 power plants and to people within 25 miles of a nuclear plant.

TABLE 6-5 ESTIMATED AVERAGE ANNUAL RISK OF ILLNESS FROM VARIOUS ACCIDENTS IN THE U.S.

Accident Type	Individual Risk Injury Probability/Year
Motor Vehicles	2×10^{-2}
All non-nuclear accidents - average person	3×10^{-2}
Very risk-averse person	3×10^{-4}
Nuclear Accidents[(a)]	1×10^{-8}

(a) This is based on early and latent illness involving the approximately 15 million people located within 25 miles of nuclear power plants.

TABLE 6-6 ANNUAL ACCIDENT FATALITIES AND INJURIES IN THE U.S.

	Total United States		People Within 25 Miles of Nuclear Sites	
Accident Type	Fatalities	Injuries	Fatalities	Injuries
Automobile	55,000	5×10^6	4200	375,000
Falls	20,000	1×10^6	1500	75,000
Fire	7,500	0.3×10^6	560	22,000
Other	33,000	1.6×10^6	2500	120,000
TOTAL	115,000	7.9×10^6	8760	592,000
Reactor Accidents (for 100 plants from Table 5-6, Chapter 5)	7×10^{-2}	1	3×10^{-3}	2×10^{-1}

TABLE 6-7 U.S. ECONOMIC LOSSES FROM VARIOUS CAUSES

Source	Estimated Annual Losses (Millions of $)
Automobile Accidents (1970)	5,000
Fires (Property - 1970)	2,200
Hurricanes (1952-72 average)	500
Fires (Forest - 1970)	70
Tornadoes (1970)	50
Reactor Accidents from 100 plants (See Table 5-6, Chapter 5)	2

TABLE 6-8 CONSEQUENCES OF MAJOR U.S. HURRICANES (1900-1972) [a]

No.	Date (month/year)	Fatalities (U.S. only)	Damage Range In Million $
1.	8/00	6,000	5 - 50
2.	9/28	1,836	5 - 50
3.	9/19	787	5 - 50
4.	9/38	600	50 - 500
5.	8/35	408	5 - 50
6.	6/57	390	50 - 500
7.	9/09	350	0.5 - 5
8.	8/69	323	500 - 5000
9.	8/15	275	5 - 50
10.	9/15	275	5 - 50
11.	9/26	243	50 - 500
12.	8/55	184	500 - 5000
13.	6/72	122	500 - 5000
14.	10/54	95	50 - 500
15.	8/65	75	500 - 5000
16.	8/54	60	50 - 500
17.	8/60	50	50 - 500
18.	8/40	50	0.5 - 5
19.	9/47	51	50 - 500
20.	9/61	46	50 - 500
21.	9/44	46	50 - 500
22.	8/32	40	5 - 50
23.	8/33	40	5 - 50
24.	9/64	38	50 - 500
25.	8/55	25	50 - 500
26.	9/54	21	5 - 50
27.	9/33	21	0.5 - 5
28.	10/44	18	50 - 500
29.	9/56	15	5 - 50
30.	9/67	15	50 - 500
31.	7/70	13	50 - 500
32.	7/34	11	0.5 - 5
33.	9/55	7	50 - 500
34.	6/16	7	0.5 - 5
35.	6/34	6	0.5 - 5
36.	10/35	5	5 - 50
37.	8/64	5	50 - 500
38.	9/41	4	5 - 50
39.	9/45	4	50 - 500
40.	10/50	4	5 - 50
41.	9/48	3	5 - 50

TABLE 6-8 (Continued)

No.	Date (month/year)	Fatalities (U.S. only)	Damage Range In Million $
42.	8/49	2	50 - 500
43.	9/49	2	5 - 50
44.	9/50	2	0.5 - 5
45.	10/35	2	0.5 - 5
46.	10/47	1	0.5 - 5
47-51.	Five others	0	5 - 50
	TOTAL 51	TOTAL 12,577	TOTAL ~ 12 Billion

(a) From "Some Devastating North Atlantic Hurricanes of the 20th Century", U.S. Department of Commerce.

TABLE 6-9 CONSEQUENCES OF MAJOR U.S. EARTHQUAKES (1900 - 1972)[(a)]

Date	Place	Fatalities	Damage (millions)
1906	San Francisco, California	~750	400
1925	Santa Barbara, California	13	6.5
1933	Long Beach, California	102	45
1935	Helena, Montana	4	3.5
1940	Imperial Valley, California	9	5.5
1949	Olympia, Washington	8	20
1952	Kern County, California	11	48
1954	Eureka, California	1	1
1957	San Francisco, California	0	1
1959	Hebgen Lake, Montana	28	4
1964	Anchorage, Alaska	125	310
1965	Puget Sound, Washington	6	12
1969	Santa Rosa, California	0	7
1971	San Fernando, California	58	480

(a) See Reference 2.

TABLE 6-10 FATALITIES IN MAJOR AIRPLANE CRASHES THROUGHOUT THE WORLD (1960-1973)

Number of Fatalities	Number of Crashes
50 - 100	40
100 - 150	21
150 - 200	6

TABLE 6-11 EARLY FATALITIES IN MAJOR EXPLOSIONS THROUGHOUT THE WORLD (1925-1971)

Fatalities	Number of Explosions	Probability of Event Per Year in U.S. With Fatalities > N	
9 - 50	30	N=8	0.47 $year^{-1}$
50 - 100	4	N=50	0.13 $year^{-1}$
100 - 200	4	N=100	0.087 $year^{-1}$
200 - 1000	3	N=200	0.043 $year^{-1}$
Largest (1100)	1	N=1000	0.01 $year^{-1}$

TABLE 6-12 DAM AND LEVEE FAILURES IN THE U.S. (1889-1972)

Year	Name/Location	Type of Structure	Lives Lost
1889	/Johnston, Pa.	Dam	~2000
1890	Walnut Grove/Prescott, Ariz.	Dam	150
1894	Mill River/Mass.	Dam	143
1900	Austin/Austin, Pa.	Dam	8
1928	St. Francis Dam/Ca.	Dam	~450
1955	/Yuba City, Ca.	Levee	~38
1963	Baldwin Hills/Los Angeles, Ca.	Reservoir	5
1972	/Buffalo Creek, W. Va.	Dam	125
1889-Present		Total	2919

TABLE 6-13 ANNUAL RATES OF FIRES WITH LARGE ECONOMIC LOSSES

Dollar Loss	Annual Frequency (approximate average)
>1 million	50
>3 million	14
>10 million	3
>20 million	1.2
>40 million[(a)] (4 in 8 years)	0.5

(a) Includes 3 large forest fires estimated at 40-50 million each and 1 large industrial fire at 75 million.

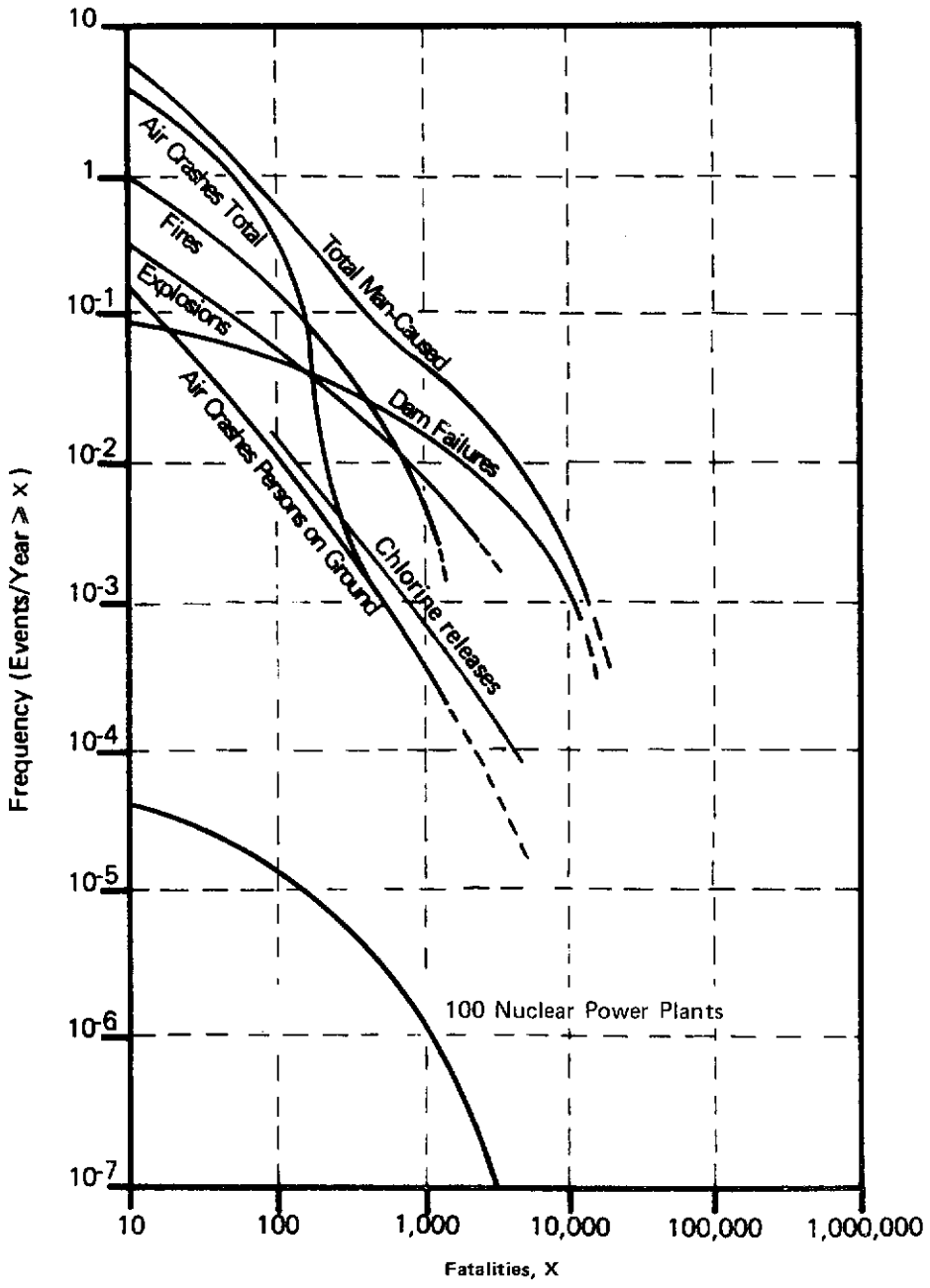


FIGURE 6-1 Frequency of Man-Caused Events Involving Fatalities.

Notes:

1. Fatalities due to auto accidents are not shown because data are not available for large consequence accidents. Auto accidents cause about 50,000 fatalities per year.
2. See section 6.4 for a discussion of confidence bounds applicable to the non nuclear curve. See section 5.5 for the confidence bounds on the nuclear curve.

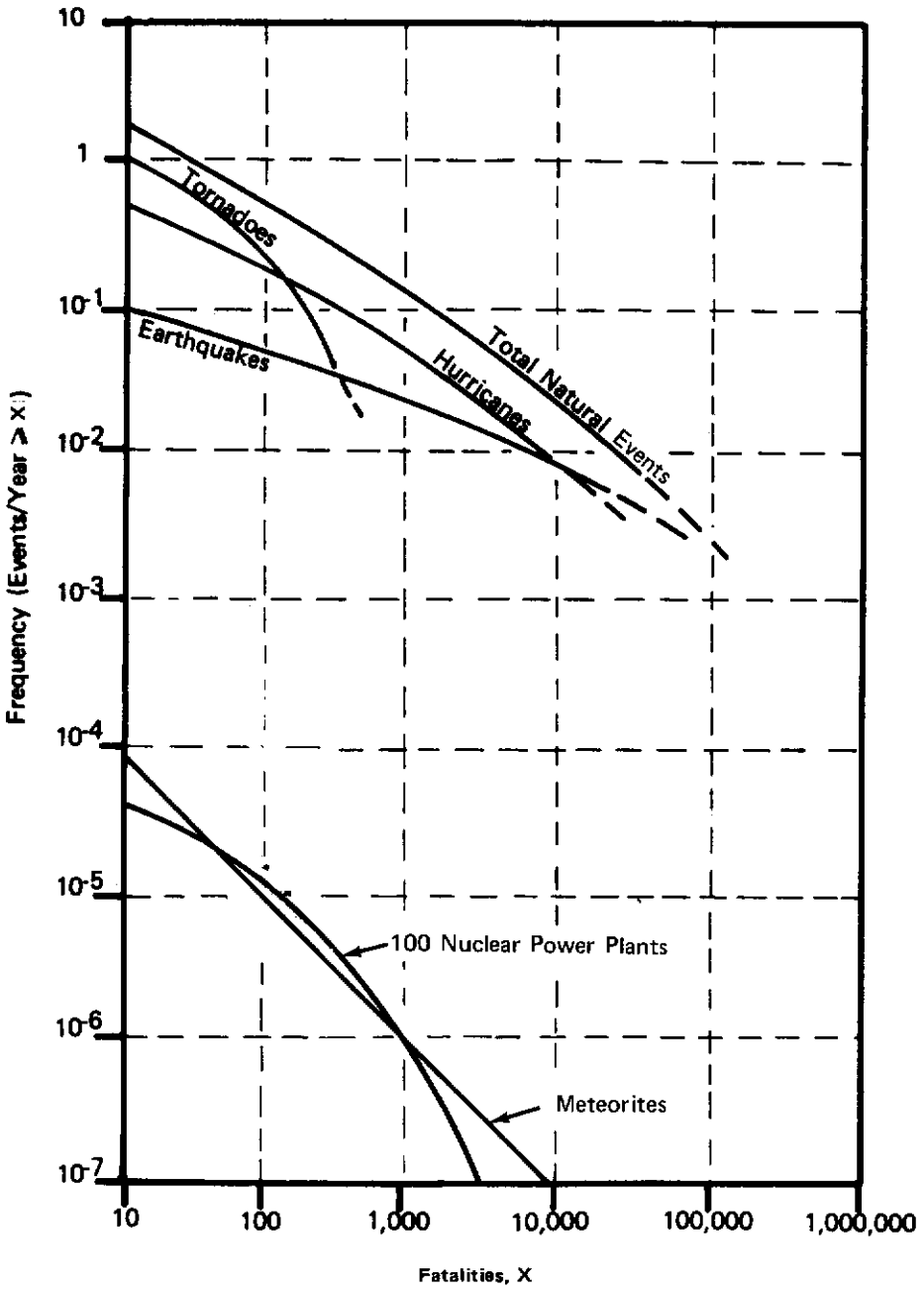


FIGURE 6-2 Frequency of Natural Events Involving Fatalities.

Note: See section 6.4 for a discussion of confidence bounds applicable to the non nuclear curve. See section 5.5 for the confidence bounds on the nuclear curve.

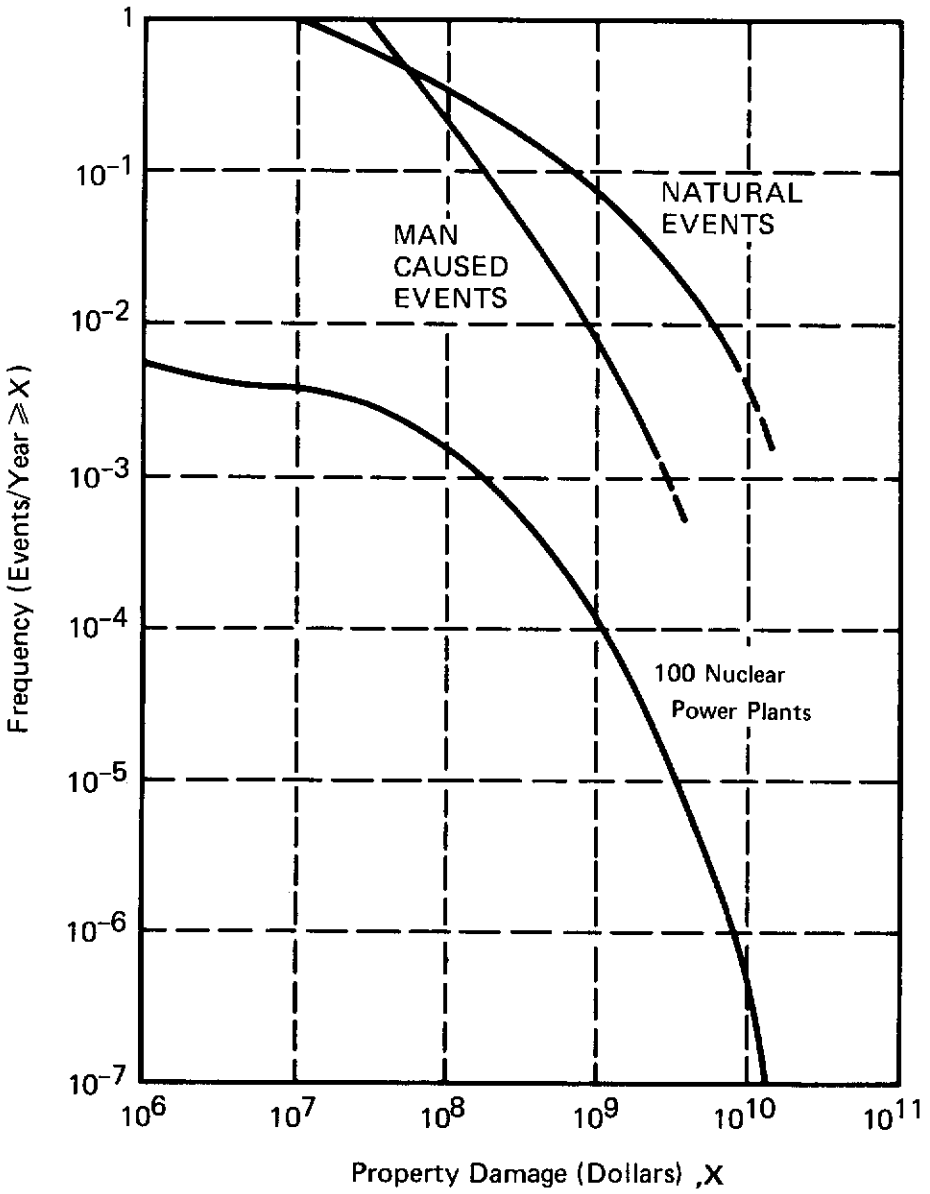


FIGURE 6-3 Frequency of Accidents Involving Property Damage

Notes:
1. Property damage due to auto accidents is not included because data are not available for low probability events. Auto accidents cause about $15 billion damage each year.
2. See section 6.4 for a discussion of confidence bounds applicable to the non nuclear curve. See section 5.5 for the confidence bounds on the nuclear curve.

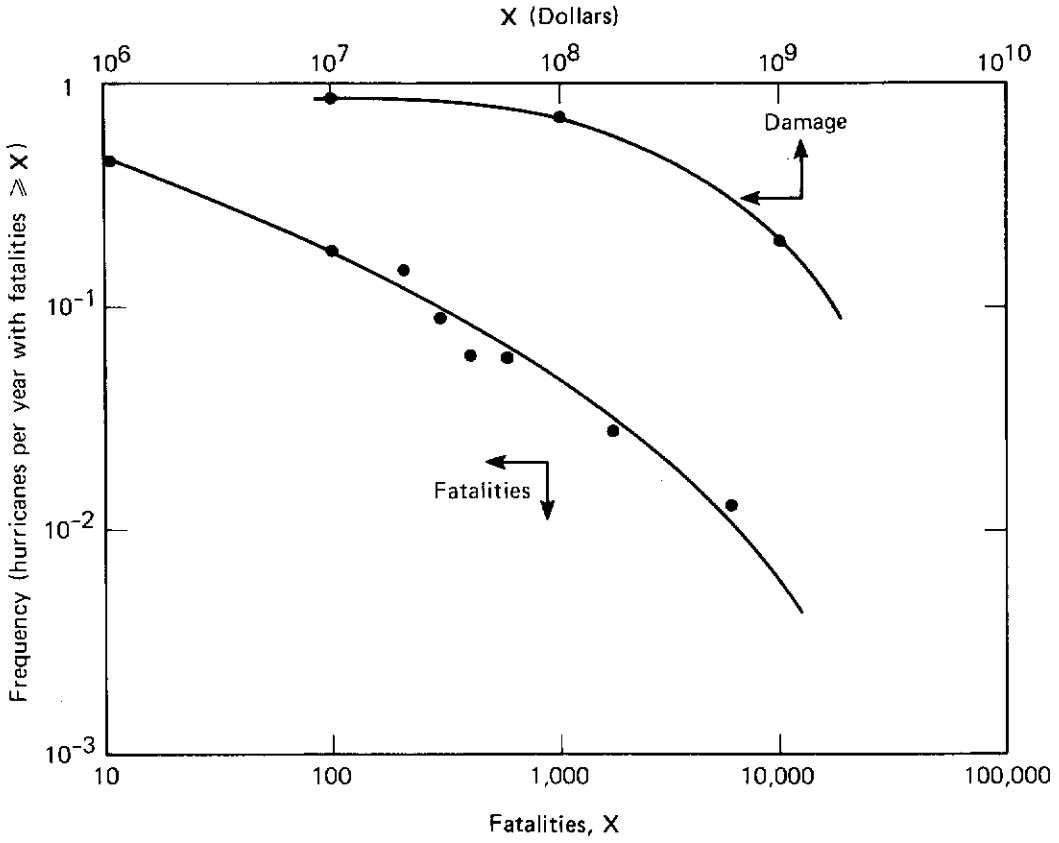


FIGURE 6-4 Frequency of Hurricane Consequences

Note: See section 6.4 for a discussion of the confidence bounds applicable to these curves

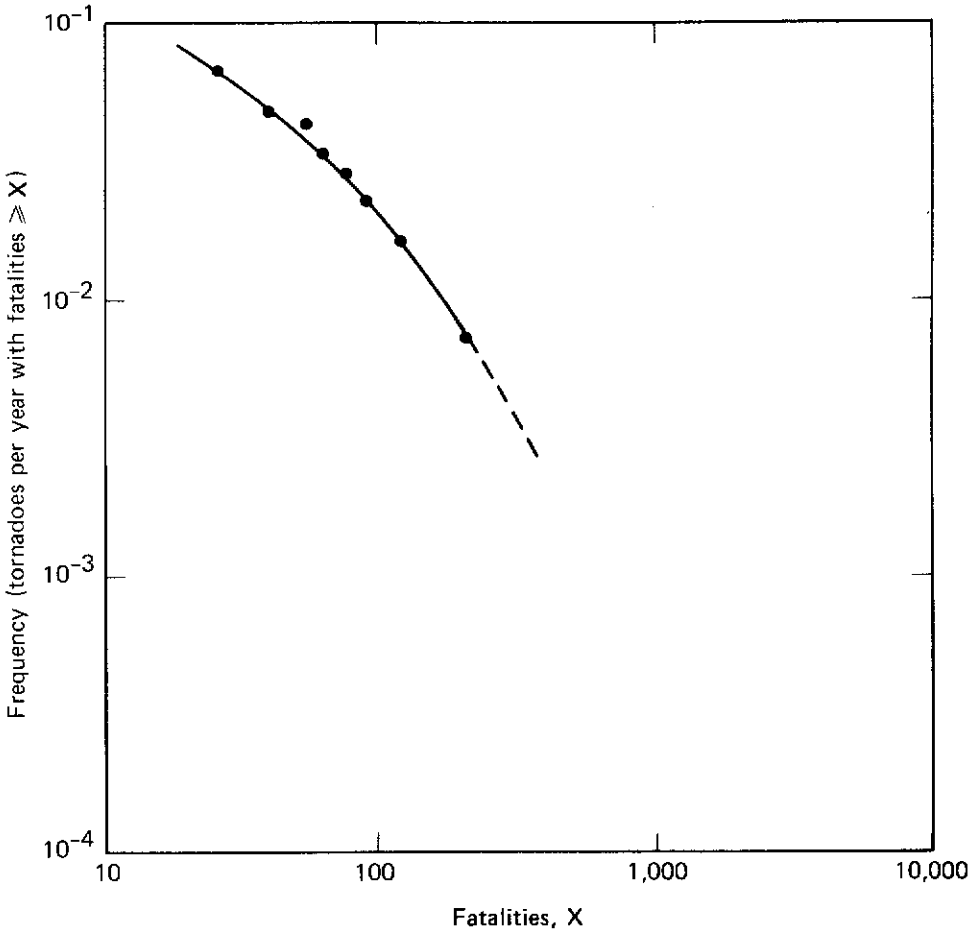


FIGURE 6-5 Frequency of Tornado Consequences

Note: See section 6.4 for a discussion of the confidence bounds applicable to these curves

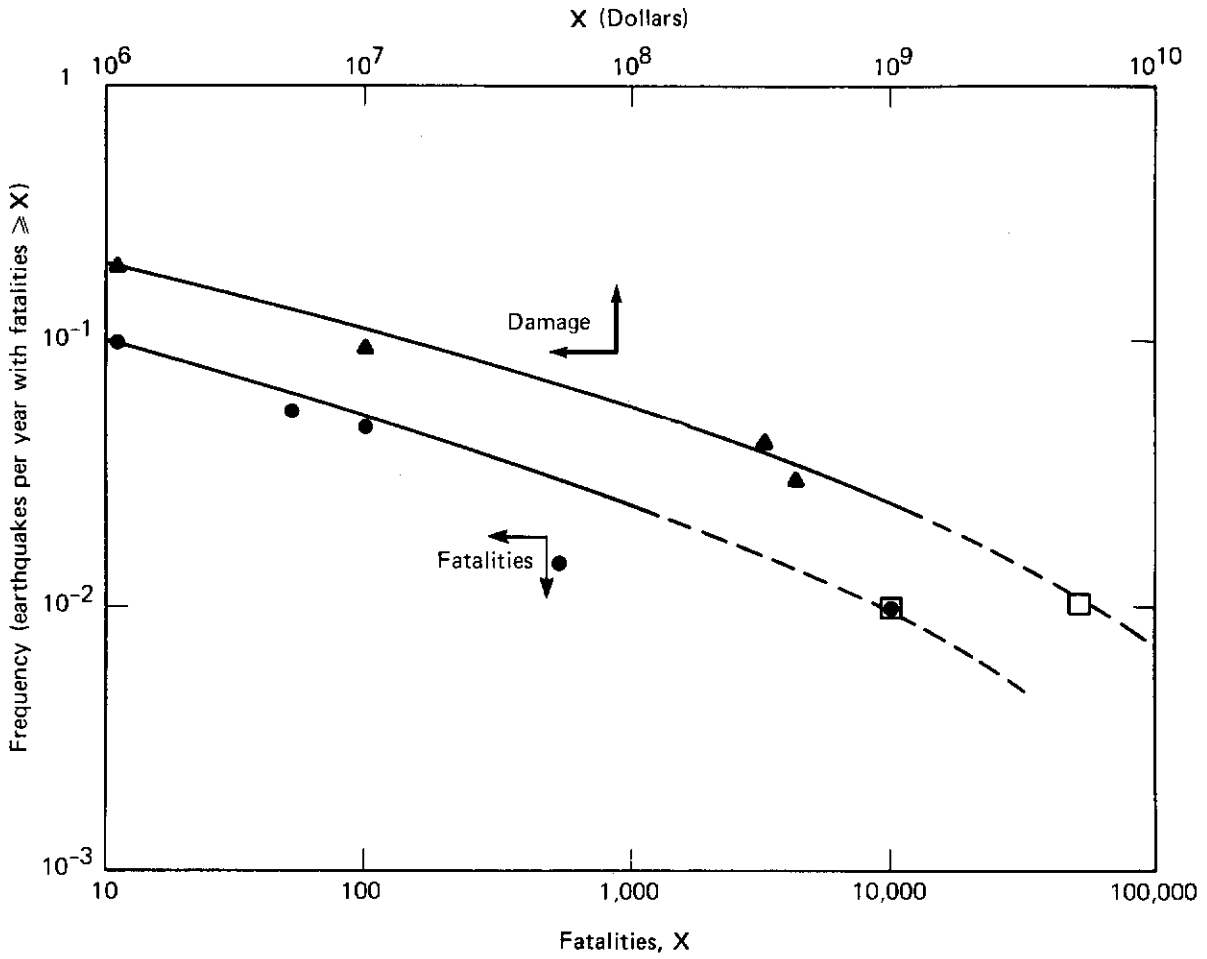


FIGURE 6-6 Frequency of Earthquake Consequences

Note: See section 6.4 for a discussion of the confidence bounds applicable to these curves

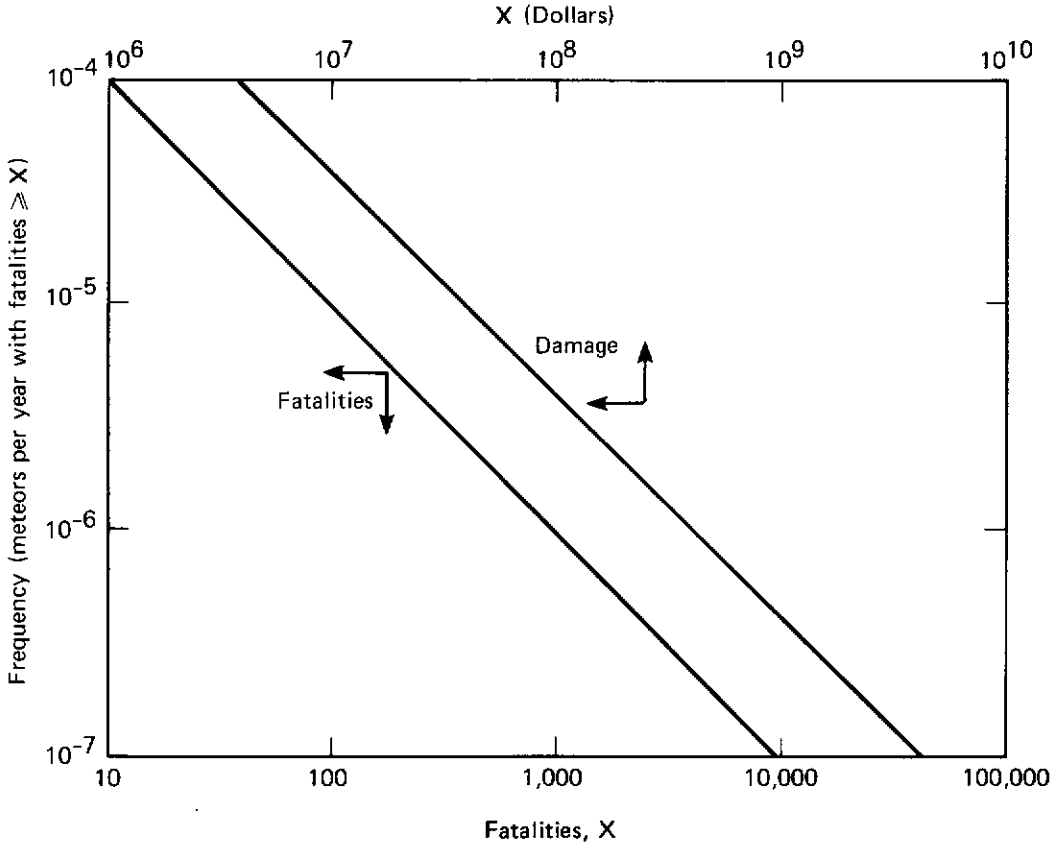


FIGURE 6-7 Frequency of Meteorite Consequences

Note: See section 6.4 for a discussion of the confidence bounds applicable to these curves

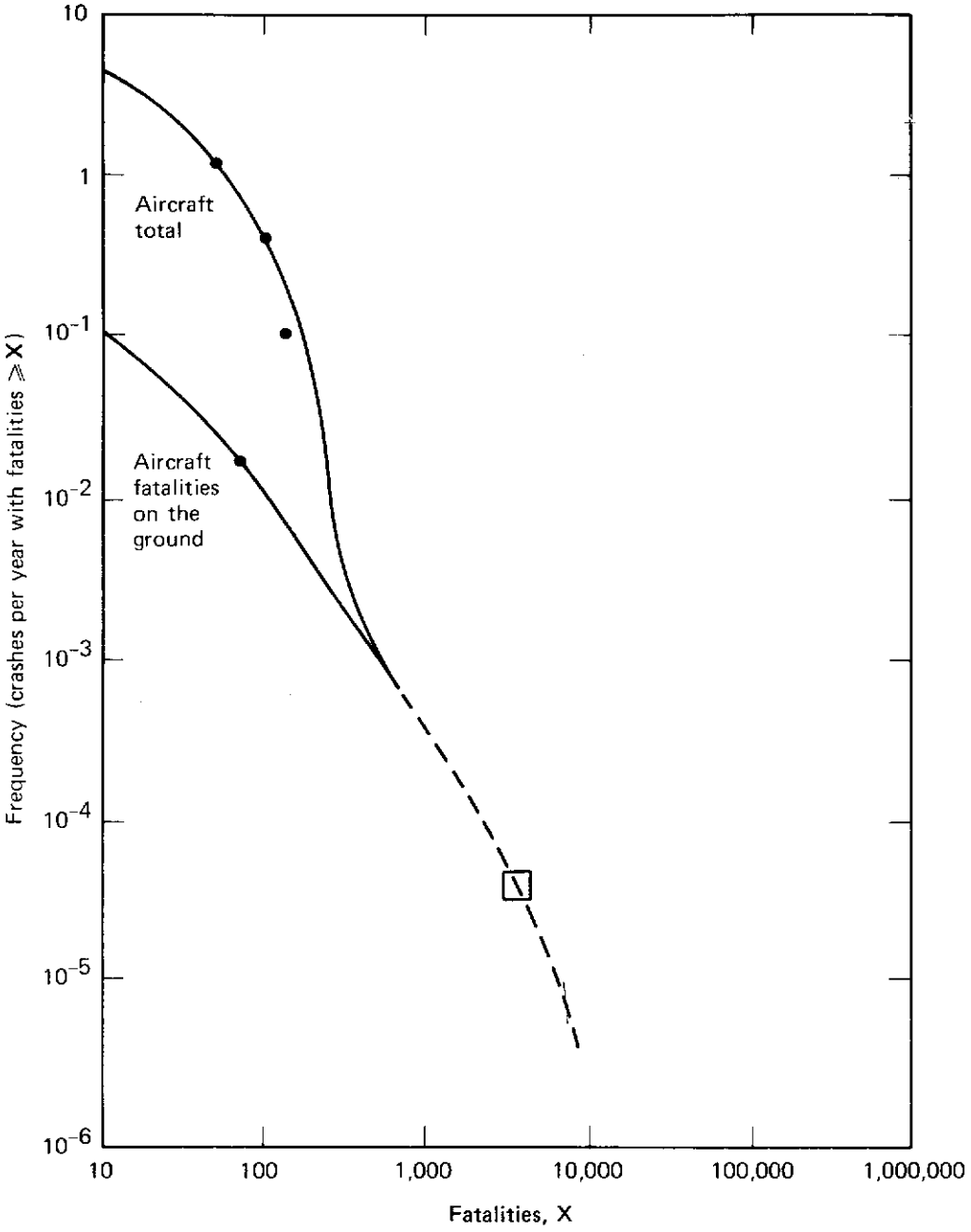


FIGURE 6-8 Frequency of Airplane Crash Consequences

Note: See section 6.4 for a discussion of the confidence bounds applicable to these curves

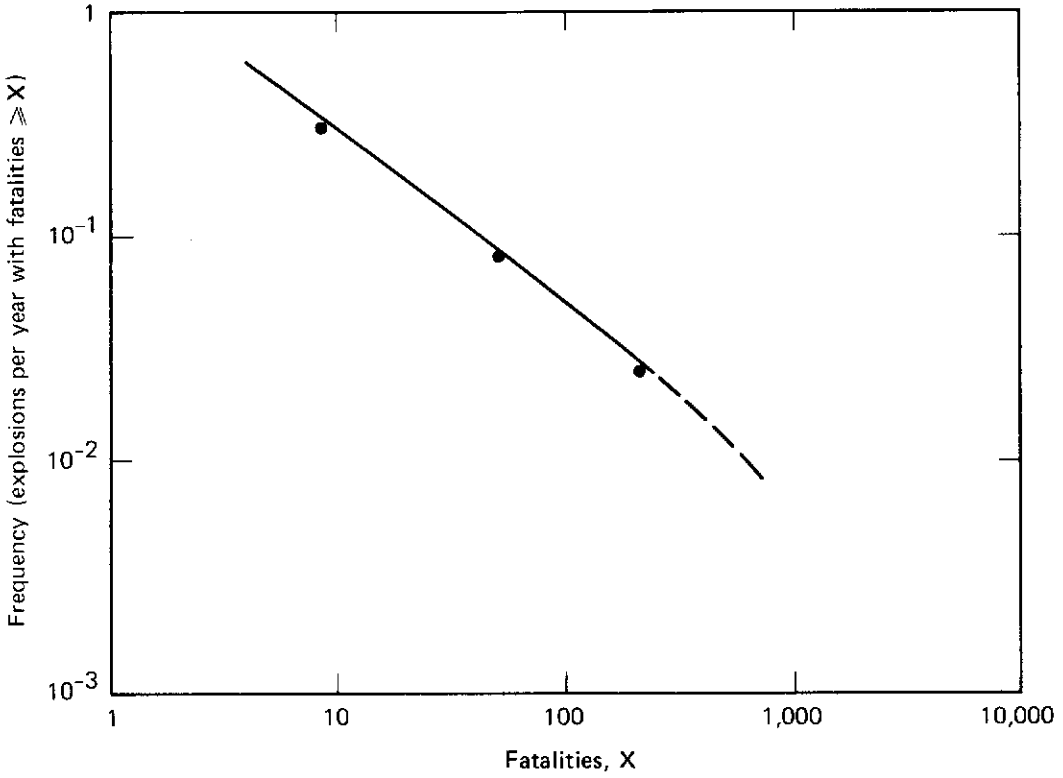


FIGURE 6-9 Frequency of Explosion Consequences

Note: See section 6.4 for a discussion of the confidence bounds applicable to these curves

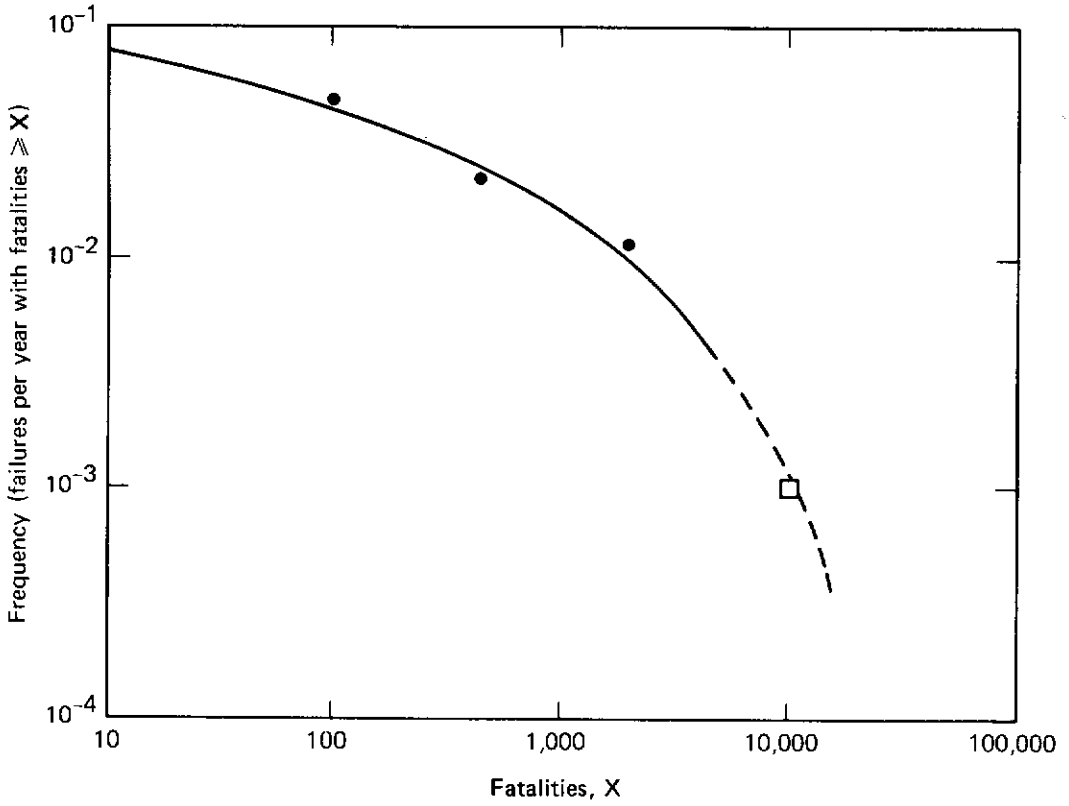


FIGURE 6-10 Frequency of Dam Failure Consequences

Note: See section 6.4 for a discussion of the confidence bounds applicable to these curves

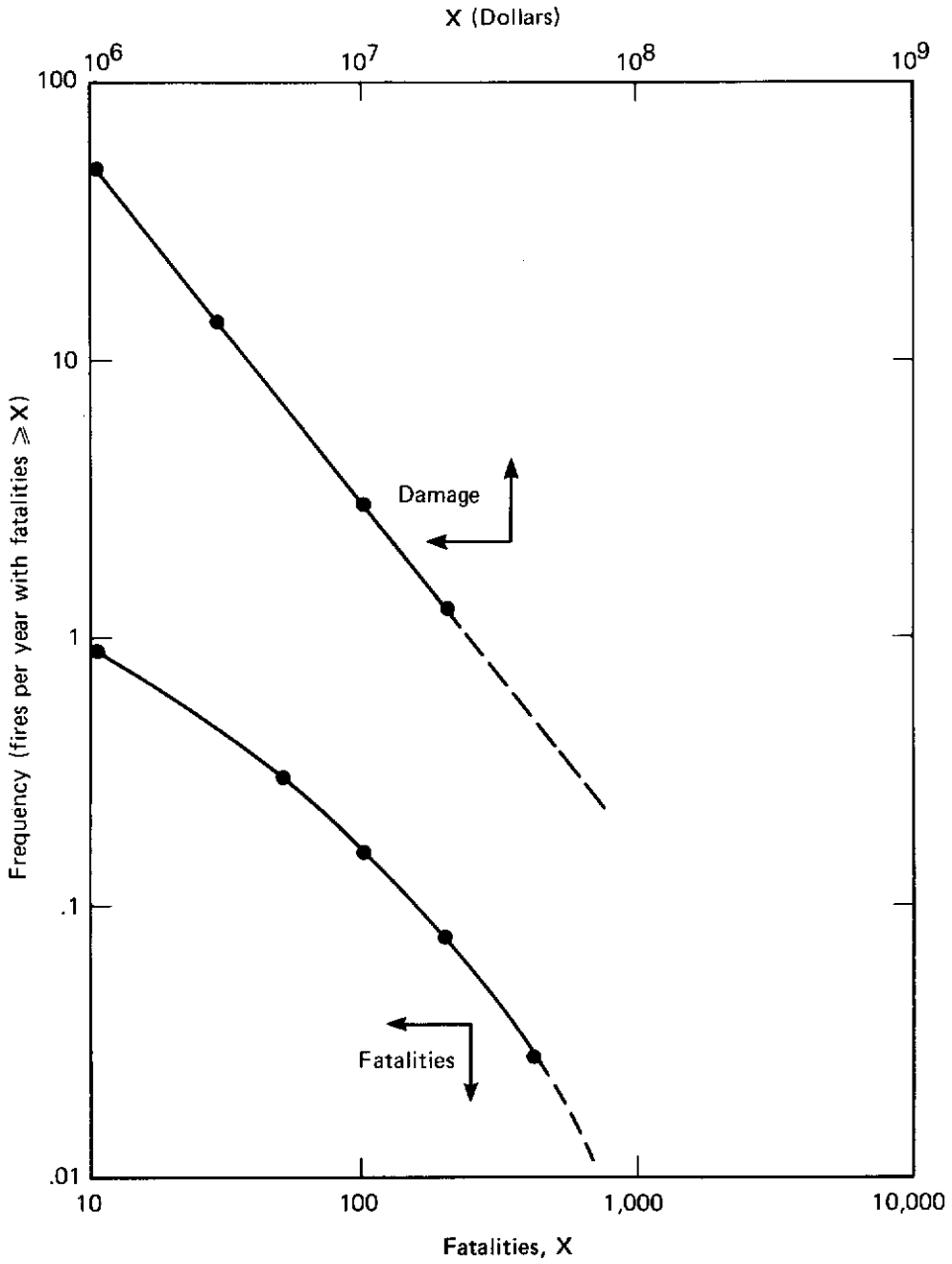


FIGURE 6-11 Frequency of Fire Consequences

Note: See section 6.4 for a discussion of the confidence bounds applicable to these curves

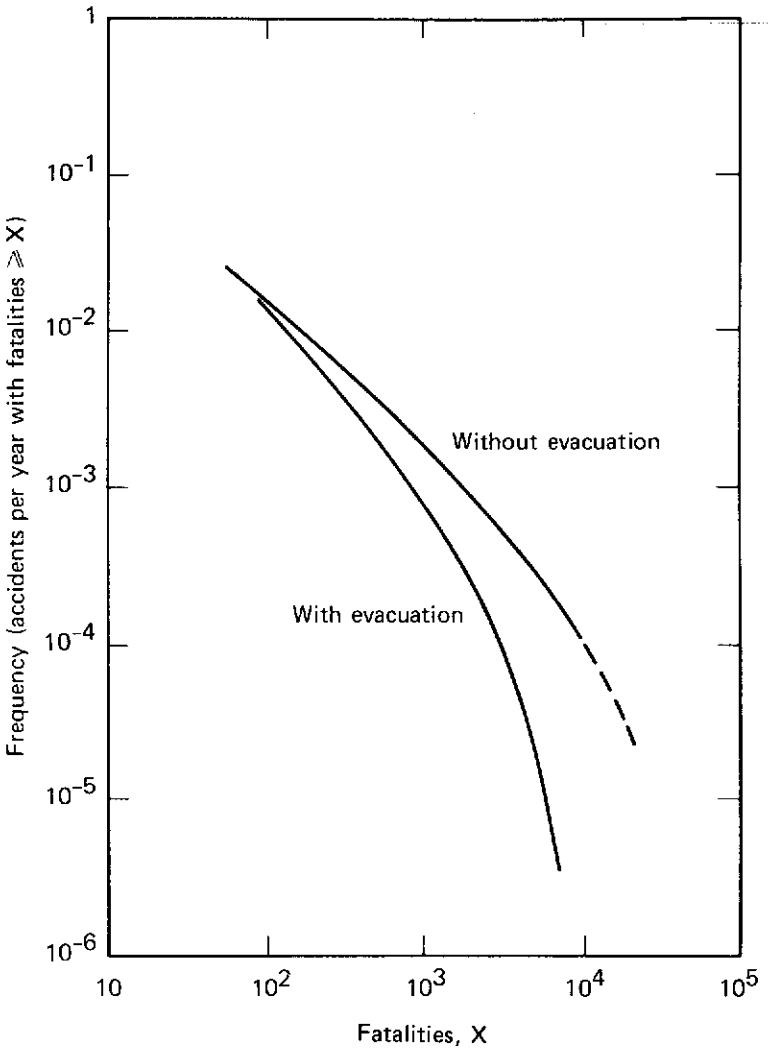


FIGURE 6-12 Frequency of Chlorine Accidents Involving Fatalities

Note: See section 6.4 for a discussion of the confidence bounds applicable to these curves

Chapter 7

Conclusions and Recommendations

7.1 OVERVIEW

The results of the Reactor Safety Study indicate that nuclear power plants have achieved a relatively low level of risk compared to many other activities in which our society engages. Although the study has developed some insights that contribute to a better understanding of reactor safety, the existing low level of risk has been achieved principally by the efforts of industrial design, construction and operation and by the efforts of the AEC's regulatory process. There will be a tendency for many in industry and government, at both working and management levels, to attempt to use various aspects of this work in connection with the safety design, operation, and review of nuclear power plants. Although the methodology used in the study has the potential to be useful for this purpose, care should be exercised before plunging headlong into such an effort.

Many of the techniques involved are deceptively simple in appearance and relatively new in their application. Furthermore, the overall model used in the study has been directed only toward risk assessment. Consequently, many elements were developed and implemented only toward that purpose; thus, they are not directly applicable for other purposes such as optimization of safety designs and the determination of effects of reactor accidents at individual sites. The use of models for purposes such as these will require further development by those who wish to perform analyses other than overall risk assessment.

Decision making processes in many fields, and especially in safety, are quite complex and should not lightly be changed. This is especially true where a good safety record has already been obtained, as is so far true for nuclear power plants. As pointed out in Chapter 2, the use of quantitative techniques in decision making associated with risk is still in its early stages and is highly formative. While these techniques can be used now as another effective tool to help decision making processes, it appears that, for the near future, additional methodological development is needed in quantitative techniques before they can be used routinely.

One of the first questions that arises about the results of the study concerns its applicability to reactors other than those studied. There are those who will question the extension or results beyond the two reactors involved in the study; there are also those who will try to extrapolate the results to 1000 reactors. The reactors studied are the 24th and 34th large reactors to come into operation. Their designs were started in 1966. The 100th plant is expected to come into operation in about 1981; its design started in about 1971. The 1000th plant is not yet a concept; nor is it clear that 1000 water reactors of the types studied will be built.

By the same token, the first 100 plants, although they involve some detailed differences in design, all meet similar safety requirements and generally have the same types of engineered safety features. Thus, the extrapolation of these results to 100 reactors seems fairly reasonable. It will also tend to overestimate rather than underestimate the risks involved, because significant improvements were made in AEC's safety design requirements, in the implementation of these requirements, and in the applicable codes and standards used in the design of nuclear power plants in the years between 1966 and 1971.

The study devoted a significant effort to ensuring that it covered the potential accidents important to the determination of public risk. In its analysis of potential nuclear power plant accidents, the Reactor Safety Study relied heavily on the twenty or more years of experience that exists in the analysis of reactor accidents. It also went considerably beyond the conventional analyses performed in connection with the licensing of reactors by considering failures that are not normally covered in standard safety evaluations. Thus, in addition to defining the various initiating events that might potentially cause accidents, the study estimated the likelihood and consequences of the failure of the various engineered safety features provided to prevent accidents and to cope with the consequences of accidents. Failures of reactor vessels and steam generator vessels as potential accident initiators were considered. The availability of systems to remove decay heat from a shutdown reactor was

examined as an additional part of the assessment of transient events. The likelihood that various external forces might cause reactor accidents was also taken into account.

The following factors provide a high degree of confidence that the significant accidents have been included: 1) the identification of all significant sources of radioactivity located at nuclear power plants, 2) the fact that a large release of radioactivity can occur only if reactor fuel melts, 3) knowledge of the factors that affect heat balances in the fuel, and 4) the fact that the mechanisms that could lead to heat imbalances have been scrutinized for many years. This confidence also rests on a number of additional factors such as:

a. the use of event trees to systematically define and screen thousands of conceivable accident sequences to identify those that are potentially possible and to determine the dominant contributors to risk.

b. the development of fault trees for engineered safety systems to a level of great detail to identify potential system failure modes and system interdependencies.

c. the determined effort devoted to the identification of potential common mode failures that had a large effect on increasing the predicted likelihood of the accident sequences defined in event trees and that also had some effect on increasing the predicted likelihood of system failures.

While there is no way of proving that all possible accident sequences that contribute to public risk have been considered in the study, the systematic approach utilized in identifying possible accident sequences and their dependencies make it very unlikely that a contributor has been overlooked that would significantly change the risk estimate.

7.2 RESULTS OF THE RISK ASSESSMENT

The quantitative results of the risk assessment that has been performed can be summarized as follows:

a. Reactor risks are predicted to be smaller than many other man-made and natural risks to which we are exposed as a society and as individuals. These other risks include those due to fires, explosions, dam failures, air travel, toxic chemicals, tornadoes, hurricanes and earthquakes. Figures 6-1, 6-2 and 6-3, taken from Chapter 6 and reproduced here for the convenience of the reader, predict that the operation of 100 reactors will not contribute measurably to the overall risks due to acute fatalities and property damage from either man-made or natural causes.

b. Table 6-3, also reproduced here, shows the average annual risks from many man-made and natural causes. The risks from potential nuclear plant accidents are smaller than the others listed both on a societal and individual basis.

c. Figures 6-1 - 6-3 do not show effects such as early illness, latent illness, genetic effects and latent

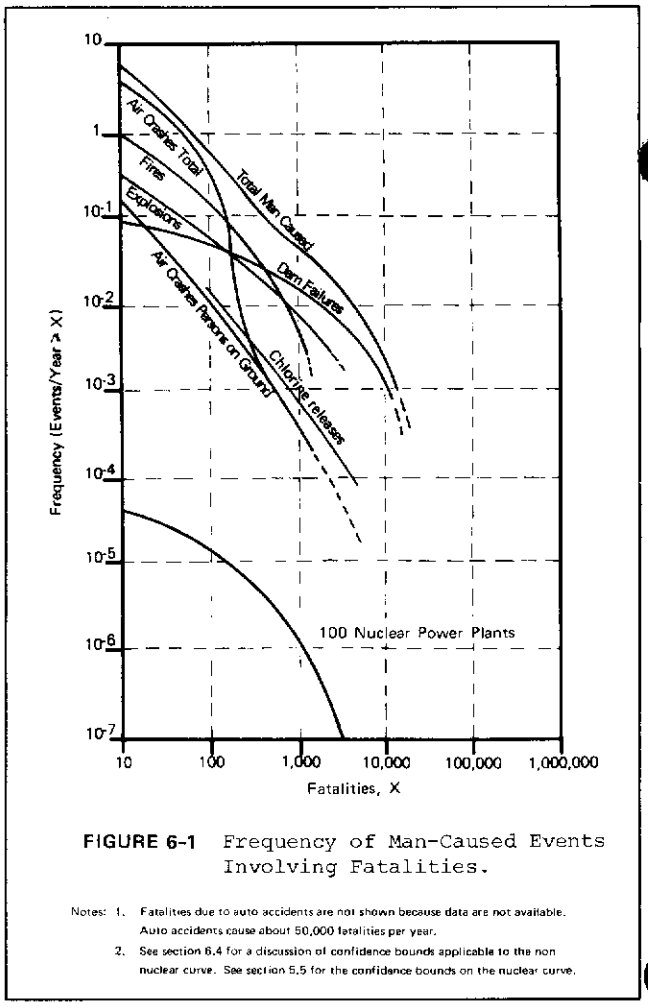


FIGURE 6-1 Frequency of Man-Caused Events Involving Fatalities.

Notes: 1. Fatalities due to auto accidents are not shown because data are not available. Auto accidents cause about 50,000 fatalities per year.

2. See section 6.4 for a discussion of confidence bounds applicable to the non nuclear curve. See section 5.5 for the confidence bounds on the nuclear curve.

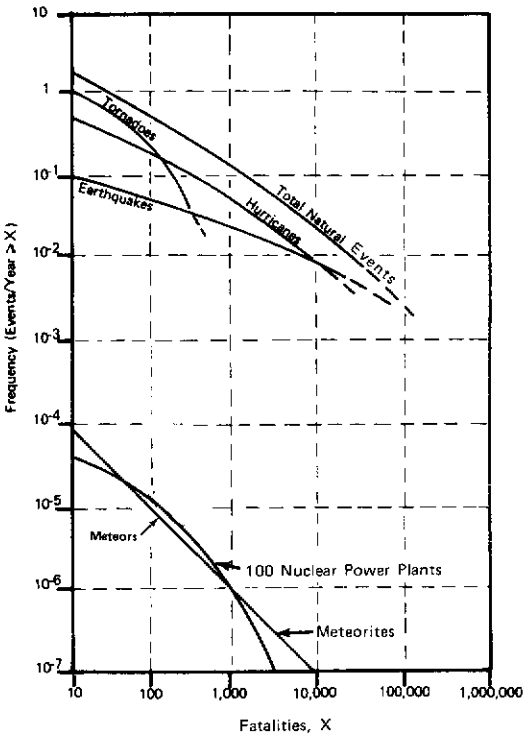


FIGURE 6-2 Frequency of Natural Events Involving Fatalities.

Note: See section 6.4 for a discussion of confidence bounds applicable to the non nuclear curve. See section 5.5 for the confidence bounds on the nuclear curve.

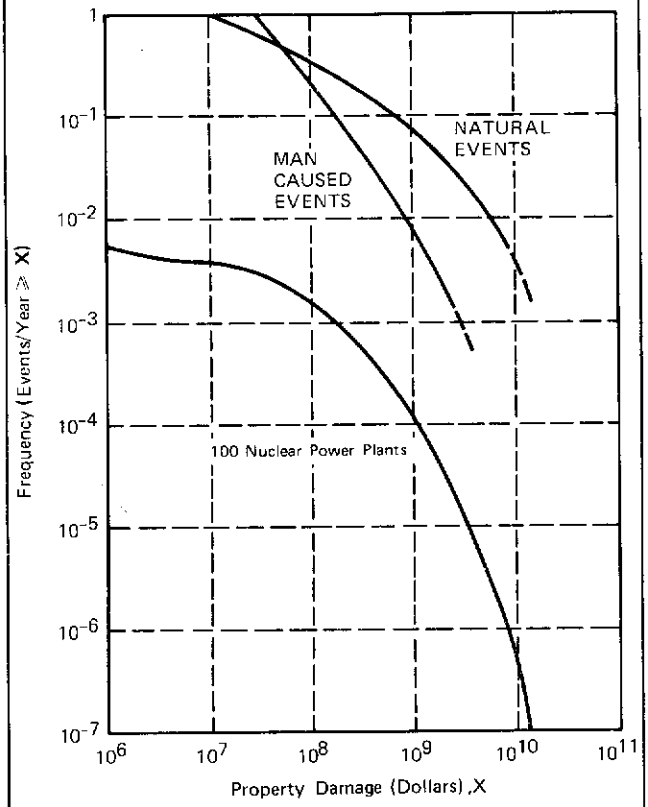


FIGURE 6-3 Frequency of Accidents Involving Property Damage

Notes:
1. Property damage due to auto accidents is not included because data are not available for low probability events. Auto accidents cause about $15 billion damage each year.
2. See section 6.4 for a discussion of confidence bounds applicable to the non nuclear curve. See section 5.5 for the confidence bounds on the nuclear curve.

cancer fatalities. Such effects have been calculated for reactors and are shown in Table 7-1. Since similar data are not available for the quantification of these types of risks from other man-made activities or natural causes, no comparisons can be made between nuclear and non-nuclear risks in these areas. However, it should be noted that these types of risks are also caused by these other sources. For example, some latent health effects can occur as a result of physical injuries and their associated diagnostic X rays.

Some perspective on the meaning of the values shown in Table 7-1 can be gained from the following considerations:

Early Illnesses. There are 8 million serious injuries in the U.S. every year due to accidents of all kinds. As shown in Table 7-1, early illness due to reactor accidents are negligible by comparison.

Delayed Health Effects. Delayed health effects that could occur due to potential reactor accidents include latent cancer fatalities, thyroid nodules, and genetic effects. The predicted occurrence rates of these effects for a population of 100 reactors are presented in Table 7-1. The predicted rates that would result from reactor accidents are also compared to the normal incidence rates for these effects in a number of people comparable to that which would be exposed to a reactor accident. Table 7-1 indicates that latent cancer fatalities and genetic effects would be a small percentage of the normal incidence rates of these effects and would probably not be discernable. In the largest accident, thyroid nodules would be approximately equal the normal rate and would be discernable. Further,

TABLE 6-3 INDIVIDUAL RISK OF FATALITY BY VARIOUS CAUSES
(U.S. Population Average 1969)

Accident Type	Total Number for 1969	Approximate Individual Risk Early Fatality Probability/yr[a]
Motor Vehicle	55,791	3×10^{-4}
Falls	17,827	9×10^{-5}
Fires and Hot Substance	7,451	4×10^{-5}
Drowning	6,181	3×10^{-5}
Poison	4,516	2×10^{-5}
Firearms	2,309	1×10^{-5}
Machinery (1968)	2,054	1×10^{-5}
Water Transport	1,743	9×10^{-6}
Air Travel	1,778	9×10^{-6}
Falling Objects	1,271	6×10^{-6}
Electrocution	1,148	6×10^{-6}
Railway	884	4×10^{-6}
Lightning	160	5×10^{-7}
Tornadoes	118[b]	4×10^{-7}
Hurricanes	90[c]	4×10^{-7}
All Others	8,695	4×10^{-5}
All Accidents (from Table 6-1)	115,000	6×10^{-4}
Nuclear Accidents (100 reactors)	—	2×10^{-10}[d]

(a) Based on total U.S. population, except as noted.
(b) (1953-1971 avg.)
(c) (1901-1972 avg.)
(d) Based on a population at risk of 15×10^{6}.

the rates due to reactor accidents are temporary and would decrease with time. The bulk of latent cancer fatalities, and thyroid nodules would occur in a period of a few decades. The rate of incidence of genetic defects would decrease substantially in five generations.

Table 7-1 shows, for example, that there is one chance in 10,000 per year of having an accident that will have 300 or more early illnesses as a consequence. Normalized on a core melt basis, this one chance in 10,000 is equivalent to 2 out of any 100 core melts producing these consequences.

d. In addition to effects already discussed, other potential effects of reactor accidents include contamination of land and water. Above various thresholds of contamination, it would become necessary to relocate people, decontaminate land of radioactivity, monitor crops and milk for contamination and possible confiscation, and perhaps interrupt use of water supplies.

People would have to be evacuated from certain areas after severe reactor accidents. This can be thought of in terms of initial relocations with return of some of the people after decontamination procedures were carried out, with a small residual area remaining evacuated for a longer period. These predicted evacuation areas are indicated in Table 7-2.

The areas in which crops and milk might be affected are about 5 and 50 times greater respectively than the initial relocation area. The affected crop areas apply for one growing season; they would be smaller thereafter. Iodine contamination would affect milk supplies for only 1 or 2 months until the iodine decays to acceptable levels.

The effects of potential contamination of water supplies have not been considered in detail in the study. If streams and rivers are contaminated to levels of radioactivity above drinking water tolerances, the use of the water would be restricted during the short time that contaminated water would flow past water supply intakes. Contamination of a water supply reservoir would require that an alternate supply be used until the radioactive levels decayed to drinking water levels or until the city water supply could be adequately filtered or treated to achieve acceptable levels. Contamination of a large lake or reservoir that represented the major water supply to a city would require restrictions on its use until levels were suitably low or until proper treatment could be implemented. It is believed that the property damage values calculated for land would cover the costs of additional water treatment should it be required.

7.3 FACTORS AFFECTING THE RISK

This study concluded that the risks from reactor accidents were dominated by those potential accidents that lead to melting of the reactor core. A variety of other accidents were examined, but their predicted consequences contribute a negligible amount to the public risk. It was found that several factors contributed importantly in the risk calculations. These included the probability of occurrence of the following factors: 1) core melt, 2) the amount of radioactivity released, 3) weather conditions, and 4) population exposed.

7.3.1 PROBABILITY OF CORE MELT

This study determined the probability of core melt to be about 5×10^{-5} per reactor year. This value is somewhat higher than a number of estimates, that have often been quoted, of 10^{-6} per reactor year. This is due to the fact that contributions to the overall risk from loss of coolant accidents (LOCAs) due to small ruptures in the reactor coolant system and from transient events are predicted to lead to core melt with a higher likelihood than those of large LOCAs. The probability of core melt due only to large LOCAs is predicted to be about a factor of 10 less than that of the dominant accidents, or about 5×10^{-6}.

In the pressurized water reactor, small LOCA accident sequences were determined to be important contributors to the core melt probability. However, other events (such as transients initiated by loss of offsite power followed by failure of decay heat removal systems) also contributed to the core melt probability. The small LOCA sequences when combined statistically with other contributing paths to core melt gave the total probability for core melt of about 6×10^{-5} per reactor-year.

In the boiling water reactor, the major contributors to core melt probability were found to be the failure to rapidly shutdown the reactor when needed or failure of the decay heat removal systems after transient-caused shutdowns. The total probability of core melt for the BWR is about 3×10^{-5} per reactor-year.

It is interesting to note that failure of reactor vessels, steam generators, or missiles from pump flywheel and turbine rotor failures made essentially no contribution to the overall risk assessment. In fact, although the probability for gross rupture of reactor vessels was estimated to be 10^{-7} per vessel-year, the failure probability would have to be about 100 times more likely (i.e., about 10^{-5}) for it to contribute significantly to the overall risk assessment. Furthermore, various external forces such as earthquakes, tornadoes, hurricanes, floods, tidal waves and airplane crashes have been found not likely to affect the overall risk assessment because of the safety design requirements used for nuclear power plants in these areas.

The core melt probability for the PWR (6×10^{-5}) and the BWR (3×10^{-5}) combine to give an average value of 5×10^{-5} per reactor-year for the predicted probability of core melt. Additional perspective can be gained about the meaning of these predictions from the following considerations:

a. Counting commercial and military power reactors, there have been almost 2000 reactor-years of experience with no nuclear accidents affecting the public. This suggests that the likelihood of accidents should be less than 10^{-3} per reactor-year.

b. Examination of accident experience in many fields suggests that large accidents occur with much lower frequency than small accidents. This can be inferred from the many consequence curves shown in Chapter 6 for both man-made and natural events. It is thus reasonable to expect similar behavior in reactor accidents. Since power reactors of the type studied have not yet had even small accidents, or situations that have resulted in abnormally high fuel temperatures, this again suggests that core melting should be much less likely than 10^{-3} per reactor-year and that larger accidents should have an even smaller frequency.

Based on these arguments it is reasonable to believe that the core melt probability of about 5×10^{-5} per reactor-year predicted by this study should not be significantly larger and would almost certainly not exceed the value of 3×10^{-4} which has been estimated as the upper bound for core melt probability.

7.3.2 LARGE CONSEQUENCE ACCIDENTS

Potential core melt accidents, occurring under typical or average values of radioactive release, weather, and exposed population, would have modest consequences. The reason that probabilities are much smaller for large consequence events is that all the factors affecting consequences must be at or near their worst condition. Thus, they require a core melt accident coupled with additional failures that cause large radioactive releases coupled with unfavorable weather conditions and a very high population density exposed to the released radioactivity. Since the accident, the population, and the weather are generally independent, large consequence events are quite unlikely.

7.4 OTHER STUDY OBJECTIVES

In addition to performing an assessment of the risks involved in potential reactor accidents, the study had several other objectives that are discussed in the following paragraphs.

7.4.1 REALISM VERSUS CONSERVATISM

The study took a realistic approach as opposed to the conservatively oriented safety approach taken in the licensing process for nuclear power plants. While the overall risk model developed here is closer to realism than previous models used, it is felt that it is necessarily somewhat on the conservative side of realism. The factors that contribute to greater realism in the model include:

a. The use of event trees to define the dependencies between safety functions, the dependencies between these functions and engineered safety systems and the dependencies between the various engineered safety systems.

b. The determination of the relationship between a molten core and the probability and consequences of containment failure modes.

c. The assessment of probabilities of system failures based on contributions due to human error, testing and maintenance, and the definition of contributions due to potential common mode failures.

d. The use of a consequence model that contains probability distributions for population and weather conditions as well as provisions for the effects of evacuation and plume rise.

e. The use of more realistic failure definitions for various safety functions (such as containment failure pressure) in areas where this could be done.

f. The use of more realistic values for factors affecting the efficiency of removal of radioactivity by means of natural deposition, sprays and filters.

g. The use of more realistic dosimetry and dose-response relationships in the prediction of health effects; in particular, the use of dose rate and dose magnitude dependency, as opposed to the linear hypothesis, in the prediction of latent cancer fatalities.

Factors that may make the model conservative are:

a. Radioactive release definitions were based on experiments having large surface to volume ratios which enhances the release of radioactivity. In a reactor the molten fuel would have much smaller surface to volume ratios that would likely cause significantly smaller releases.

b. Some parameters in the calculation of the transport and removal of radioactivity in containment were in general conservatively applied.

c. Conservative values were selected for the individual isotopic releases among those accident sequences which dominated the likelihood of the various release categories discussed in Appendix V. This, in combination with items a. and b. above, yielded high values of releases of radioactivity.

d. Although a plume rise model was used that allowed sensible heat released from the containment to cause the plume to lift off the ground initially (thereby reducing near plant exposures), the model did not account for latent heat that was also released or for internal radioactive heating of the plume. Inclusion of these heat sources might have reduced the predicted early health effects.

e. Although the handling of weather effects included the time variation of weather stability, wind speed, and rain, the effects of wind shear and changes in wind direction were not included. Also the treatment used for rain effects may be conservative. The net effect of this approach may make the model conservative with regard to the predicted values for those consequences, such as early health effects, property damage, and land contamination, that are threshold dependent.

f. The assumption was made that biological effects due to radioactive exposures have effects down to very low doses.

g. The assumption that molten uranium dioxide falling into saturated water had a 10% chance of causing a steam explosion is considered to be quite conservative. Available experimental data indicates that steam explosions do not occur in saturated water.

h. As indicated earlier in this chapter, the study probably overestimates the likelihood of accidents as applied to the first 100 reactors to be operated.

7.4.2 METHODOLOGICAL DEVELOPMENTS

The many aspects of the methodological developments and approaches have been extensively discussed in the report and its appendices. Among the more important aspects of the methodological contributions to the study are:

a. The methodological approaches developed in the study include the use of event trees to determine potential accident sequences, including the dependencies involved; the propagation of error bands in the calculation of system failure probabilities, probabilities of accident sequences and of the release of radioactivity, detailed calculations of radioactive release and transport in containment, and the use of a consequence model that includes probabilistic distributions of weather conditions and population densities that are characteristic of existing reactor sites and a plume rise and evacuation model.

b. With regard to component failure rate data, it was found that existing data is sufficiently accurate to perform meaningful risk evaluations especially since the statistical propagation of variabilities in the quantification of system fault trees and event tree accident sequences permitted the use of data and their associated uncertainties from a wide variety of sources. General data sources, including data from industrial experience, could thus be integrated with nuclear data to obtain a composite, working data base which was used to quantify system failure probabilities with an accuracy adequate for risk calculations.

   It was found that existing nuclear data in itself was not sufficiently comprehensive nor sufficiently quantifiable to be used as a sole data source. The nuclear data which was available, however, has had a primary role in assessing the validity and consistency of other data sources. In the study, nuclear abnormal occurrence reports for 1972-73 and certain earlier reports, along with reactor in-plant operating experience were incorporated in the data evaluations and assessments. Error spreads associated with the data served to cover uncertainties and possible variations in the final assessed values.

   Data on human factors, e.g., reliability and error potential were found to be sparse, thus requiring some degree of subjectivity when assessing their contribution. The lack of more precise data did not, however, adversely impact the meaningfulness of the final results of the risk evaluations. The use of error spreads also served to cover uncertainties associated with this data.

   In general, the existing data had about a factor of 3 to a factor of 10 or greater uncertainties and lacked specificity as to failure categorization and failure cause. If more exact calculations are to be performed, or if decisions are necessary that require more exact calculations to assess the validity of potential system improvements, better data is then required and better data analysis needs to be implemented. It would be useful to establish a comprehensive data collection and analysis program applicable to nuclear power plants.

c. It is clear that the heart of successful risk assessment and a principal factor in determining the adequacy of event tree and fault tree methodology is the proper identification of potential common mode failures. Considerable effort was devoted to assessing the potential impact of common mode failures on the study's results. It is difficult, however, to generalize on the overall impact of common mode failures since they were found to have varying degrees of significance depending on the particular stage of the analysis. An important point to note is that attention to the potential for common mode failures was required throughout all stages of the analyses.

   Significant common mode failure impacts were found in the event tree sequences and in the analyses of containment failure modes. The common mode considerations of functional and system interdependencies resulted in significant modifications to event trees and hence in the probability values resulting for many of the event tree sequences. Because of the functional and system interdependencies, the probability

values for accident sequences resulting in core melt could in many cases be the result of single engineered safety system failures.

On the other hand, in the quantification of fault trees and event trees, while common mode failures in most cases had significant effects, they were smaller than the effects found in the event trees. In general, single system failure probabilities dominated the probability of an accident sequence and single component failures in turn dominated the system probability. When this occurred, common mode failures had little impact since at most they could change multiple independent failures into single dependent failures and these already existed. Human errors, because of their larger probabilities as compared to component failure rate data, dominated the system failure probabilities in a number of cases. In certain systems, however, common mode contributions did enter importantly, for example, when several failures were attributed to a common human interface. It would be useful to study the matter of human errors in order to be able to predict their effects with greater precision.

The conclusion that common mode failures were found to have varying significance in this study strongly indicates that for proper context, common modes and general dependency considerations should not be isolated and treated separately as has sometimes been done, but should be incorporated throughout all stages of the analysis.

d. The analyses of engineered safety system availabilities generally predicted system failure probabilities to be in the range of 10^{-4} to 10^{-2}. There were deviations from this general range in the case of a few systems having higher or lower failure probabilities. Generally, there were also a number of different contributions to system failure, involving hardware related causes, test and maintenance related causes and/or human errors. Test and maintenance and human error contributions were important factors in roughly half the systems. Common mode contributions, often involving the human, also were important in a number of systems, and particularly in redundant systems. As already mentioned, the collection and analysis of failure rate data and the further study of human errors would be useful in improving the precision of potential system failures probabilities.

e. The use of fault trees in their current state of development is time consuming and expensive. While they are a useful tool in predicting the failure probabilities of engineered systems, it would be useful to systematize their application in order to make their utilization more efficient.

In addition to the factors of realism and the factors that still make the model somewhat conservative as discussed earlier, there are also a few elements of uncertainty in the model.

a. As discussed in Chapter 5, the seismic design adequacy (that is the adequacy of the implementation of seismic design requirements in the detailed plant design) was found to be deficient in some areas. Although the logic presented there supports the view that seismic events as large or larger than those chosen for the design basis should not contribute significantly to the accident risk, it is somewhat surprising that a greater degree of confirmation of seismic design adequacy could not be obtained. Part of this could be due to the fact that seismic design requirements were relatively new at the time these plants were designed and part could be due to the after-the-fact nature of the review by this study. It would be helpful to study this matter further on more recent plants.

b. As already mentioned, the risk assessment performed in the study is based on two light water cooled nuclear power plants. There may be some variations in design from reactor plant to plant as well as from site to site which could potentially affect the applicability of the results obtained. It would be useful to pursue these matters further to give a greater degree of confidence in the extrapolation of results to other plants and to develop the techniques for making individual site calculations. It would also be useful to repeat an overall WASH-1400 type risk assessment for water reactors in about 5-10 years.

c. The study could not completely cover the risks due to potential acts of sabotage because no convincing way could be found to estimate the prob-

ability of acts of sabotage directed at any target. However an investigation of this area has led the study to the conclusions that nuclear power plants are difficult to sabotage successfully, that acts of sabotage are not expected to lead to consequences more severe than the maximum predicted by the study and that nuclear power plants are far less susceptible to sabotage than most other targets. Furthermore, improvements have recently been made in plant security and further requirements are under consideration. With the implementation of current security measures, it appears that the probability of successful sabotage is low and further reductions in probability can be anticipated in the future.

d. The probabilistic treatment of the various input parameters to the consequence model has not been carried out uniformly in this study. However, parametric studies have been performed that establish a reasonable basis for the estimated error bands used in the study. The development of a consequence model that incorporates the additional probabilistic elements that may be needed would be useful.

e. The consequence model assumed evacuation of population from the area that could potentially be affected by accidents in which the core melts. It also assumed that some warning would be given in advance of the actual release of radioactivity. Although nuclear plants are already required to have plans for evacuation in the case of potential accidents, the importance of evacuation in reducing accident consequences suggests that steps be taken to ensure that the communications, instrumentation and monitoring needed to provide adequate evacuation warning are provided. It would also be useful to study potential alternatives for achieving dose amelioration effects.

f. As discussed in Chapter 5, although the potential contribution to reactor accident risks due to floods and fires do not affect the predicted risks importantly, it would be useful to perform additional analysis to define their potential contribution to risk on a more broadly applicable basis.

7.4.3 RESEARCH SUGGESTIONS

As indicated earlier there are some areas in which the availability of additional data would help to determine the degree of conservatism in the risk estimates performed. The suggestions below do not address overall safety research; they cover only those areas that could be of help in risk assessment studies.

1. Release of Radioactivity from Molten Fuel. Data on radioactive releases that would be expected to occur from molten fuel having a small surface to volume ratio would be of use in making the overall risk assessment more realistic.

2. Steam Explosions. Although data from small scale experiments indicate that molten metals and water do not interact in an explosive way with saturated water, the study has permitted this possibility because of the unknowns associated with potentially large scale events. Further experimental data would be useful to determine the need for this conservatism.

3. Heated Plumes. Further investigations of the effects on plume behavior of the various kinds of heat sources in potential reactor accident plumes would be useful.

4. Risk Assessment Development. It would be useful to continue the coherent development of WASH-1400 techniques in further improving this capability in risk assessment and in the performance of risk assessments. Fruitful areas for further risk assessment include barge mounted nuclear power plants, liquid metal fast breeder reactors, high temperature gas cooled reactors and fuel reprocessing plants.

While the areas above have been suggested as potential candidates for additional safety research, this research is not regarded as urgent since the risks from reactor accidents, as calculated in this study, indicate them to be lower than many others in society.

7.5 FINAL OBSERVATIONS

The principal insights gained in this study are:

a. Contrary to the commonly held belief that all nuclear power plant accidents involving core melting would surely result in severe accidents with large public consequences, the

magnitudes of the potential consequences of a core melt accident were found to have a wide range of values. The probability is high that the consequences would be modest compared to other types of risks. The likelihood of relatively severe consequences is quite low.

b. The consequences of reactor accidents are often smaller than many people have believed. Previous AEC studies have been based on unrealistic assumptions and have predicted relatively large consequences for reactors that were much smaller than current reactors. Consequently, there are some who believe, incorrectly, that reactor accidents can produce consequences comparable to that of the explosion of large nuclear weapons. Further, there are many in the nuclear field who have believed that accidents involving melting of the reactor core would always lead to large consequences. This study has shown that predictions of the consequences of nuclear power plant accidents, when performed on a more realistic as opposed to an upper limit basis, are smaller than previous predictions would have led one to believe and, in fact, are no larger, and often smaller, than the consequences of other accidents to which we are already exposed.

c. The likelihood of reactor accidents is smaller than that of many other accidents having similar consequences. While there are some in the public sector who will feel that the likelihood of occurrence of nuclear power plant accidents should be made essentially zero, neither nuclear accidents nor non-nuclear accidents of any kind can have zero probability. We do not now, and never have, lived in a risk-free world. Nuclear accident risks are relatively low compared to other man-made and natural risks. All other accidents, including fires, explosions, toxic chemical releases, dam failures, earthquakes, hurricanes, and tornadoes, that have been examined in this study are more likely to occur and can have consequences comparable to or greater than nuclear accidents.

d. There are many who, as a result of this study, will advocate immediate action to accomplish objectives such as changing the safety design of reactors to decrease the likelihood of the events that were the principal contributors to the risk assessment and in setting reactor safety standards based on the use of quantitative techniques. If the risks attached to nuclear power are as small as this study finds, such actions may not be necessary, and could potentially be self defeating. As already indicated, although the use of quantitative techniques in making decisions on the basis of risk is still in its beginning stages these techniques can be used effectively as another tool in aiding decision making processes. It would be wise to continue their further development to make them of greater utility in assisting decision making.

e. The question of what level of risk from nuclear accidents should be accepted by society has not been addressed in this study. It will take consideration by a broader segment of society than that involved in this study to determine what level of nuclear power plant risks should be acceptable. This study should be of some help in these considerations.

TABLE 7-1 APPROXIMATE VALUES OF EARLY ILLNESS AND LATENT EFFECTS FOR 100 REACTORS

Chance Per Year	Consequences			
	Early Illness	Latent Cancer Fatalities[b] (per yr)	Thyroid Illness[b] (per yr)	Genetic Effects[c] (per yr)
1 in 200[a]	<1.0	<1.0	4	<1.0
1 in 10,000	300	170	1400	25
1 in 100,000	3000	460	3500	60
1 in 1,000,000	14,000	860	6000	110
1 in 10,000,000	45,000	1500	8000	170
Normal Incidence Per Year	4×10^5	17,000	8000	8000

(a) This is the predicted chance per year of core melt for 100 reactors.

(b) This rate would occur approximately in the 10 to 40 year period after a potential accident.

(c) This rate would apply to the first generation born after the accident. Subsequent generations would experience effects at decreasing rates.

TABLE 7-2 LAND AREA AFFECTED BY POTENTIAL NUCLEAR POWER PLANT ACCIDENTS FOR 100 REACTORS

Chance Per Year	Consequences	
	Decontamination Area (Sq. Mile)	Relocation Area (Sq. Mile)
1 in 200	<0.1	<0.1
1 in 10,000	2000	130
1 in 100,000	3200	250
1 in 1,000,000	(a)	290
1 in 10,000,000	(a)	(a)

(a) No change from previously listed value.

ADDENDUM I

AN OVERVIEW OF EVENT TREE AND FAULT TREE METHODOLOGY AND THE HANDLING OF COMMON MODE FAILURES

Addendum I

Table of Contents

List of Tables

List of Figures

Addendum 1

An Overview of Event Tree and Fault Tree Methodology and the Handling of Common Mode Failures

Section 1

Introduction

The purpose of this addendum is to present an overview of the methodology used in WASH-1400 to assist the reader in judging its inherent adequacy as well as the adequacy of its implementation. Much of the material presented here is discussed briefly in the Main Report and in its various appendices. However, significant additional information and interpretive analyses are also presented.

There has been considerable discussion of the capability of such methodologies to produce reliable quantitative estimates of the probability of occurrence of system failures and of low-probability events. Much of this discussion appears to be based on the results of some early efforts that produced quite unrealistic quantitative predictions. Another aspect of these discussions concerns the ability to estimate the occurrence of low-probability events with confidence. These matters and others are covered in this addendum.

The study believes that the results obtained in WASH-1400 represent a significant extension in the application and quantification of event trees and fault trees. The material presented in this addendum attempts to define the bases for this belief and is arranged as follows:

- Section 2 discusses the adequacy of the overall methodology in general terms.
- Section 3 discusses the adequacy of fault tree methodology in general terms.
- Section 4 covers the handling of potential common mode failures in the overall risk assessment, including the contributions made by event trees and fault trees.
- Section 5 discusses the completeness of consideration of potential reactor accidents, covering those involving the reactor core as well as those involving radioactivity stored in other locations.
- Section 6 covers the handling of failure rate data in the overall risk assessment.
- Section 7 presents modeling considerations for event trees and fault trees.
- Section 8 summarizes the discussion.

Section 2

Adequacy of the Overall Methodology

This section presents a general discussion of the factors that concern some people with respect to the adequacy of WASH-1400 methodology and describes some of the reasons for these concerns. The principal factors involved are:

a. whether event tree and fault tree methodology is capable of predicting accident and system failure probabilities,

b. whether the capability exists to properly define common mode (or dependent) failures,

c. whether all potential accident sequences have been identified, and

d. whether adequate failure rate data was available to quantify fault trees.

Item a, regarding the capability of fault tree methodology to produce useful predictions of system failure probabilities, is somewhat understandable in view of the results of some early attempts to quantify fault trees. In these cases, failure to achieve useful results generally rested on one or more factors, such as the inclusion of only hardware failures in the trees and the use of an inadequate failure rate data base. Also, in some cases, higher degrees of precision were sought than were achievable, and these efforts were classed as being inadequate. Since the earlier attempts, however, considerable work has been done to improve the methodology to overcome these deficiencies. The study believes that the fault tree methodology as used in WASH-1400 produced meaningful results. Sections 3 and 4.2 discuss the adequacy of fault tree methodology.

Items b through d suggest that the methodology used in the study might not have been capable of producing meaningful and complete descriptions of all conceivable reactor accident sequences or meaningful predictions of their likelihood of occurrence. There appears to be some opinion that the lack of capability to define common mode failures adequately will prevent the successful identification of all accident sequences as well as the quantification of fault trees.

It is important to understand that the Reactor Safety Study does not purport to have included in its results contributions from all conceivable accidents and all conceivable common modes. The important question is not whether all contributions have been included, but whether the significant contributions to risk have been included. Any final risk or probability value can be envisioned as consisting of a large number of contributions that must be combined. The goal of an analysis is to include a sufficient number of significant contributions so that the results are insensitive to further contributions. The study's event tree and fault tree methodology represents a systematic and comprehensive method to help define the significant contributions.

One of the vital elements in ensuring that all significant contributions to accidents are identified is the proper handling of common mode failures. A general perception of many scientists is that the analysis of potential common mode failures is limited principally to considerations involving dependencies among component failures within highly redundant systems. It is thought that the quantification of such potential contributions, even within a single system, cannot be done with any reasonable degree of confidence; the idea of coupling multiple systems together in accident sequences appears to them to make the handling of common mode failures almost impossibly difficult.

This perception seemed generally valid to the study when the work began because it seemed that a great many combinations of multiple-system failures would be potentially possible in the accident sequences derived from event trees. However, factors not normally considered in previous analyses began to emerge more clearly as the study progressed. These factors, at least for light water cooled nuclear power plants of the type now being built in the United States, led to the following insights about the risk assessments performed in the study:

a. There are many identifiable tightly coupled interrelationships that exist in potential accident se-

quences in these nuclear power plants. These include interrelationships among the functions to be performed, between the functions and among the systems provided to perform those functions, and the systems themselves.[1] These interrelationships, which are explicitly defined on the basis of engineering knowledge and physical principles, have the effect of reducing the number of potentially conceivable interactions by very large factors.

b. Many of the accident sequences defined by event trees involved the failure of only single systems as opposed to multiple systems. Further, the failure probabilities of most of these systems involved only single failure type[2] contributions. Thus, the Reactor Safety Study accident analyses involved neither a large number of highly redundant systems nor the combinations of such systems.

c. In risk assessment, estimates of high precision are not needed. Thus, bounding and approximation techniques of many kinds can be used successfully to assess the potential impacts of common mode failures. If the results of the application of such techniques do not impact within the accuracy of the calculations, then further analysis to define potential additional common modes is not needed. Where high degrees of precision (e.g., system reliability design) are needed, such bounding techniques may not be useful.

Based on the above considerations, the proper handling of common mode failures throughout all stages of the analysis is vital in determining the significant contributors to risk and in predicting meaningful accident and system probabilities. Furthermore, there is a close relationship between the ability to define common mode failures and the ability to define the significant contributors to risk. To the extent that all significant common mode failures cannot be determined, it is not possible to say that all significant contributors have been defined. The definition of accident sequences in event trees and fault trees must therefore include extensive consideration of potential common mode failures.

Section 4 of this addendum discusses common mode failures as a complete topic, pointing out the contributions made to their identification by event trees, fault trees, and the statistical techniques used in their quantification. Section 5 examines the way in which the study determined the accident sequences of significance. Section 6 describes the data base used in the quantification of the event trees and fault trees.

---

[1] See section 2 of Appendix I for a more complete description of these interrelationships.

[2] A single failure type of contribution has a probability equal to that of a single component (hardware) failure, single human error, or single test and maintenance contribution.

Section 3

Adequacy of the Fault Tree Methodology

There have been statements made in recent years that challenged the conceptual adequacy of fault tree methodology. One of the principal points of these statements was that fault tree analysis is incomplete and is unable to produce reliable quantitative predictions of system failure. It has been asserted that the National Aeronautics and Space Administration (NASA) and the aerospace industry abandoned use of the fault tree technique for this reason. The major reasons cited for the supposed deficiencies in fault tree methodology include the following:

a. Fault trees cannot identify all potential causes of system failure and hence yield underestimates of system failure probability.

b. Fault trees are subjective because the analyst must decide which events are to be incorporated into the trees and which events are to be omitted.

c. The results of the quantification of fault trees cannot be relied on because insufficient failure data are available.

To obtain a balanced perspective in discussing these areas, it is instructive to review those viewpoints that support the adequacy of fault tree methodology before proceeding.[1]

A letter of June 16, 1975, from the Administrator of the National Aeronautics and Space Administration to the Chairman of the U.S. Nuclear Regulatory Commission indicates NASA's current view of the study's methodology.[2] In summary, the NASA letter states that the event tree and fault tree methodology used in the Reactor Safety Study is an effective technique and is capable of producing numerical assessments of value if the data base from which failure probabilities are determined has sufficient accuracy and content that is applicable to the quantification being performed. It goes on to say that, although NASA uses similar methodology, it does not use the numerical portion of the analysis because of the small data base applicable to specific NASA projects.

Mr. A. E. Green, General Manager of the Systems Reliability Service (SRS) in England and coauthor of the text Reliability Technology, has also provided his views of this matter[3] (Ref. 1). The SRS group has been using reliability techniques for a number of years, and Mr. Green states that the group has found the general methodology to be competent, giving predictions that are generally within a factor of 2 of achieved failure rates. In support of this realistic prediction capability, a graph is cited from Reliability Technology, which shows the close agreement the SRS group has so far experienced between predicted probabilities and observed system failure rates. The letter notes that this curve shows that, for some 50 system elements, the ratio of observed failure rate to predicted failure was within a factor of 4.

Another comment that should be cited here was contained in a letter from the U.S. Environmental Protection Agency (EPA) dated August 15, 1975. The letter is reproduced here, in part, as follows:

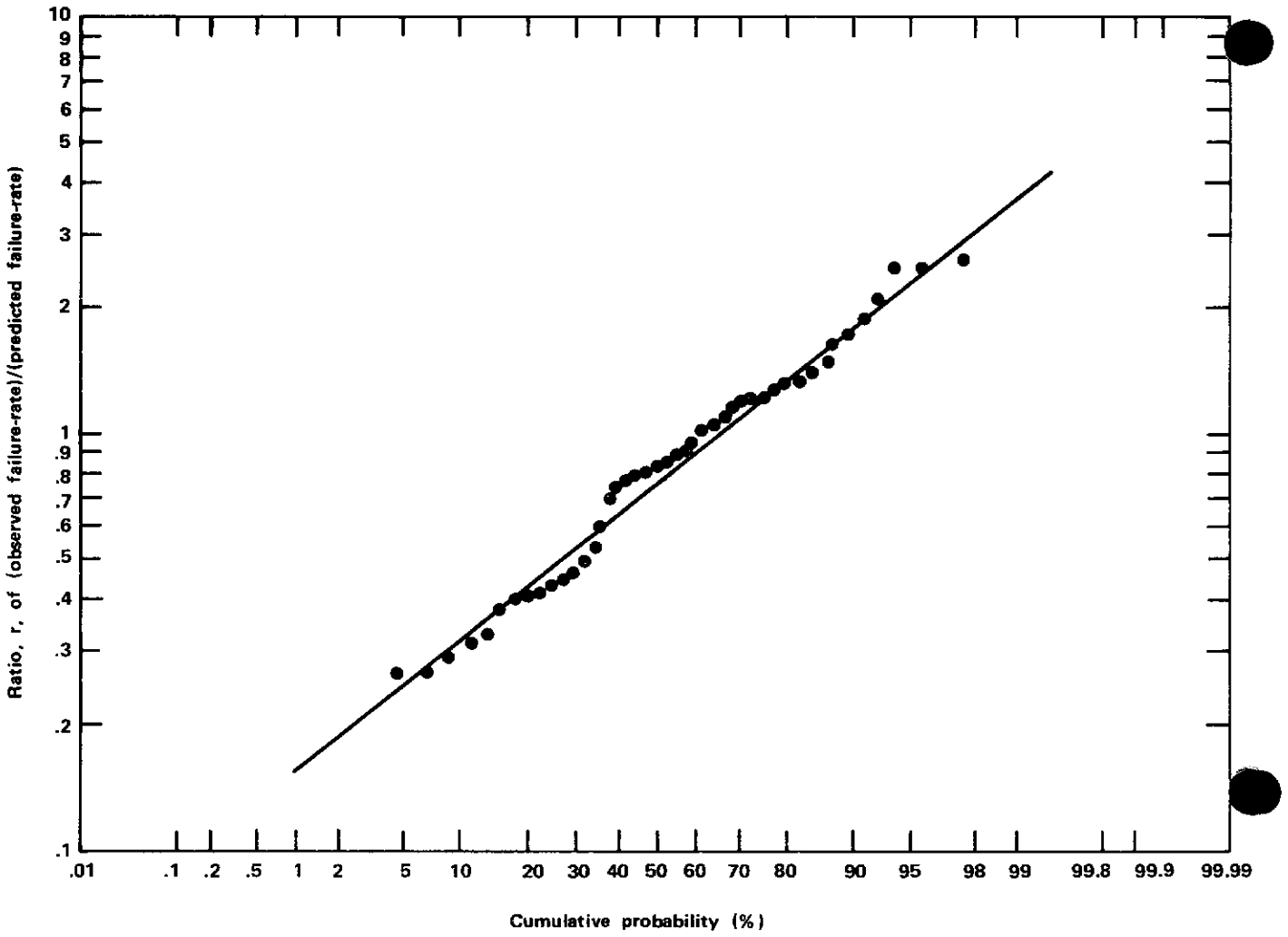
"Because of the significance of the Reactor Safety Study toward establishing the accident risk associated with nuclear power plants, we chose to review the draft report of the study in two phases. The comments from our first phase review, an overall review of the draft WASH-1400, were transmitted to you by our letter of November 27, 1974. The second phase review was an intensive examination of selected areas of draft WASH-1400 to determine if there were deficiencies in their evaluations and to estimate the significance of the deficiencies with respect to the related

---

[1] The procedures used in the study to help ensure the completeness of fault trees and to achieve their reliable quantification are described in section 4.2.

[2] This letter is appended to this addendum as Attachment 1.

[3] Mr. Green's letter is appended to this addendum as Attachment 2.



risk calculations in draft WASH-1400. This effort provided a deeper appreciation of the degree of thoroughness with which the Reactor Safety Study staff has applied the study methodology and of the sensitivity of the study results to changes in individual parameters or in single event probabilities."

. . . . .

"The results of our second phase review have not altered our opinion that the Reactor Safety Study provides a forward step in risk assessment of nuclear power reactors, and that the study's general methodology appears to provide a systematized basis for obtaining useful assessments of the accident risks where empirical or historical data are presently unavailable."

The General Accounting Office (GAO), at the request of Congress, made a review of reliability data on weapons and space systems.[1] The conclusions of this limited study are as follows:

"1. Although the basic reliability methodology is adaptable to Atomic Energy Commission (AEC) projects, DOD and NASA experience has limited usefulness in judging the validity of AEC's reliability predictions.

2. The confidence that can be placed on reliability predictions is directly related to the extent of previous testing or use of the same or similar systems.

3. Most early DOD reliability predictions are goals set for the con-

[1]The review, which was published on pages S 20775 and S 20776 of the Congressional Record on December 9, 1974, is appended to this addendum as Attachment 3.

tractors or laboratories to achieve in development and production. Most such goals are not initially achieved in operations; but equipment and component modifications, training, and experience usually result in upward reliability trends over a period of time.

4. Reliability of major new systems cannot be accurately predicted because of the many variables--materials, training, maintenance, and so forth--that are involved."

The study interprets the GAO conclusions not as a criticism of the methodologies as used in WASH-1400, but rather as a confirmation that they can, if used correctly, predict realistic system failure probabilities with reasonable confidence. The basis for this belief is that the reactor systems analyzed in WASH-1400 are not new and unique but are used in many reactors and are composed of components that are the same as, or similar to, those used in many other industrial applications.

As a final point, it should be noted that, although the current operating experience with reactors is insufficient to give measured values for system failure probabilities in all cases, sufficient system data were available to permit checking the WASH-1400 predicted failure rates for two systems against experience.[1] In these two cases, the predicted and observed failure rates were within about a factor of 2 of one another. This result gives some confidence that the fault trees and data used in WASH-1400 gave reasonably good results.

It is the view of the study that the net impact of the GAO report, the NASA letter, Mr. Green's letter, and the EPA letter is to confirm, as a matter of intellectual conviction and experience, that fault tree methodology can produce meaningful results. The preceding discussion seems to confirm that there is a fairly broadly held view that the methodology can serve its intended function of realistic reliability prediction and the limited (necessarily) checking of system failure predictions against field experience indicates that reasonably realistic results were obtained in the WASH-1400 implementation of fault tree methodology.

The procedures used in the study to help ensure the completeness of fault trees and to achieve their reliable quantification are described in section 4.2 of this addendum.

The discussion that follows in the next several sections addresses in greater detail the validity of the event tree/fault tree methodology. Although the discussion is directed principally toward the identification of potential dependencies and common mode failures, it also presents an overview that covers the general completeness of the methodology (which is closely related to the identification of dependencies), the specific techniques used to help ensure completeness, and the handling of failure data. It is hoped that this overview will provide the reader with a better comprehension of the study's methodology than did the widely scattered discussion in the draft report.

---

[1] See Appendix II, volume I, section 1.

Section 4
The Handling of Potential Common Mode Failures in Overall Risk Assessment

As is stated in WASH-1400, the heart of successful risk assessment and a principal factor in determining the adequacy of the event tree/fault tree methodology is the proper identification of potential common mode failures. The successful definition of common mode failures is necessary to help ensure that all the significant contributing accident sequences have been defined and that the probabilities of occurrence of the accident sequences have been adequately predicted. Many of those who have considered the problems associated with defining low-probability events and their likelihood of occurrence find it reasonable to question whether the capability exists to perform such a task, due principally to the uncertainties involved in the handling of common mode failures. In fact, as noted in WASH-1400,[1] this was one of the major uncertainties recognized from the beginning of the study.

In the risk assessment performed in WASH-1400, the identification of common mode failures was an integral part of the construction and quantification of event trees, of the construction and quantification of fault trees, and in the handling of failure data. Only by considering these three elements in concert (i.e., event trees, fault trees, and data) can one gain the necessary perspective concerning the validity of the handling of common mode failures and of the overall use of the methodology in WASH-1400.

4.1 EVENT TREE METHODOLOGY AND ITS CONTRIBUTIONS TO COMMON MODE FAILURE CONSIDERATIONS

As described extensively in Appendix I, an event tree begins with an initiating event, and proceeds to define the possible outcomes of such an event. These outcomes are determined by all the physically possible permutations[2] encompassed by the successful operation or failure of all the applicable systems installed in the nuclear power plant that can cope with the effects of the initiating event.[3] Thus, since all applicable systems that can affect the course of events are included, the construction of each event tree encompasses a set of potential accident sequences that is in essence complete for that initiating event. All the event trees used for the PWR reactor analyzed in WASH-1400 have, for example, encompassed approximately 130,000 potential accident sequences that could conceivably involve millions of potential common modes at the system failure level. Clearly the question of whether one can quantitatively handle such a large number of dependencies is extremely pertinent.

---

[1] See section 1.7 c of the Main Report.

[2] The methods used to ensure that "all physically possible permutations" of events are included in the event tree are discussed extensively in section 2 of Appendix I. These methods include the ordering of event tree headings in accordance with their relationship to the course of events involved in potential accident sequences and the use of conservatively selected, discrete definitions of system operability success and failure as a function of time.

[3] The reader is also referred to section 2 of Appendix I for a more complete discussion of the logic of event tree construction. It should be noted here that the event trees used in this study differ significantly from the more conventionally used decision trees. In general, decision trees are the representation of a process in which the adequacy of the tree depends principally on the skill and judgment of the analyst in properly conceptualizing the area under consideration. While this type of skill applies to some degree in the event trees developed in WASH-1400, the analyst is aided considerably because the elements of the trees are physical entities that exist in the nuclear power plant and the processes involved in the tree follow engineering and physical principles. The understanding of the details of plant design and of these physical principles aid the analyst greatly in ensuring a proper conceptualization for the reactor event trees.

Fortunately this problem has a solution since there exist logical methods for eliminating consideration of the vast bulk of these potential accident sequences and their associated dependencies. These methods are based on detailed knowledge of the design and engineering principles involved in nuclear power plants--principles that permit the elimination of physically meaningless sequences from the mathematically complete trees. As a further step, the use of probability discrimination among sequences having similar outcomes permits the further elimination of those sequences that do not contribute to the likelihood of specific outcomes. These techniques are described below.

Figures I 2-1 through I 2-8 of Appendix I show the development of LOCA event trees in which the initiating event is a pipe break (PB) and in which the functions to be performed after the pipe breaks are listed.[1,2] Figure 1 shows the possible choices of success or failure of each of the functions involved in potential LOCA accident sequences. Figure 2 is the same representation, except that the number of sequences has been reduced from those that are mathematically possible to encompass only those that are physically meaningful on an engineering basis.[3] For example, in those sequences involving core melt, since it is known that the containment will surely fail, choices on success or failure of containment integrity have been logically eliminated.[4] Further, where electric power (EP) has failed, no choices have been shown for any functions because none can operate without electric power. Where the reactor trip (RT) has failed, no choices are shown for emergency cooling injection (ECI), emergency cooling accumulator (ECR), and containment integrity (CI) because the core could melt from the reactor trip alone. Where

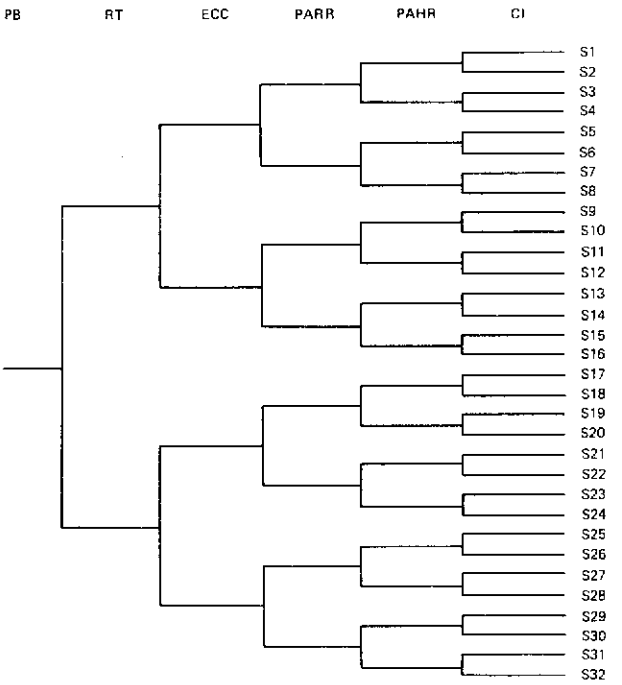


Figure 1 Illustrative Event Tree for LOCA Functions

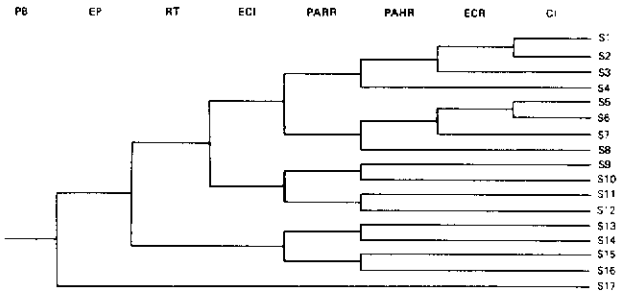


Figure 2 Functional LOCA Event Tree Showing Effects of Interrelationships

---

[1] Figures I 2-1 and I 2-8 are reproduced here for the convenience of the reader as Figs. 1 and 2 respectively.

[2] The reader is referred to section 2 of Appendix I for the definition of terms and for a more complete discussion of these event trees.

[3] A few other changes have been made, such as the addition of electric power (EP) to the tree and the substitution of emergency cooling injection (ECI) and emergency cooling recirculating (ECR) in place of emergency core cooling (ECC). This logic is explained in Appendix I, section 2.

[4] A separate event tree to define the interrelationships among, and the probabilities of, the various potential modes of containment failure is developed in section 2.2 of Appendix I.

ECI has failed, the ECR choice and CI choices are similarly of no physical significance because, again, the core would melt. Where post accident heat removal (PAHR) has failed, CI will fail due to overpressure from core decay heat and ECR will fail as a result of CI failure.

From this brief description of the engineering basis for the elimination of system choices, it can be seen that the elimination of accident sequences has not been arbitrary or judgmental, but is based on the systematic application of the engineering knowledge and principles involved in the relationships among the various systems and functions. The reduction of the event tree in Fig. 1 to that in Fig. 2 is of great importance in the handling of common mode failures and the ability of the methodology to logically reduce the analysis to a tractable size. A tree with the headings in Fig. 1, showing all possible choices of success and failure, would have yielded 128 potential accident sequences, involving 896 dependencies if all sequences were considered.[1] The application of engineering principles to this tree has trimmed it from 128 to 17 accident sequences and from 896 dependencies to 79 system-to-system dependencies.

In considering the total number of event trees involved in the overall study,[2] it can be seen that about 130,000 potential accident sequences involving millions of potential dependencies were screened to arrive at a relatively small number of remaining potential interactions that were physically meaningful and needed further investigation. This small number of interactions made it feasible to perform meaningful analyses and quantification of the remaining accident sequences. The great ability of the event trees to reduce large numbers of sequences and dependencies applies to situations involving tightly coupled systems like the nuclear systems analyzed in the study; this conclusion may not be broadly applicable to other technological designs.

A second important stage of screening and reducing potential common modes lies in considering the accident sequence outcomes (radioactive releases) and discriminating among the sequence probabilities. Accident sequences having similar releases can be grouped together and the sequence probabilities added to obtain the total probability for each of the releases. For a particular release, high-probability sequences that occur in the grouping dominate the lower probability sequences and also tend to suppress the importance of any potential common mode effects in these lower probability sequences. In summing the sequences to determine the probability of that release, only those high-probability sequences need then be retained.

Table 1 shows a list of all the 150 accident sequences derived from the combined PWR large-LOCA and containment event trees.[3] These sequences have been grouped and arranged in two ways:

a. In columns by radioactive release categories; i.e., by grouping together all sequences that would result in radioactive releases of similar magnitude.

b. By their likelihood of occurrence; i.e., the sequences shown as the dominant sequences are the ones that dominate the probability of occurrence of each release category. The sequences designated as "other" are of sufficiently low probability that they do not contribute to the sum of the dominant sequences. Bounding techniques were used in making this probability discrimination; double and triple failures were assumed to be single failures in obtaining maximum values for the sequence probabilities below the line. These maximum values were compared to the dominant sequence probabilities and were not found to impact on the dominant probabilities.[4]

Examination of the dominant sequences for all PWR event trees shows that the

---

[1] In the counting of dependencies, a sequence having n system choices is taken as having n possible dependencies.

[2] Appendix I, sections 4 and 5.

[3] Table 1 is the same as Table 3-4 of Appendix V.

[4] The criterion was that the maximum value had to be approximately two orders of magnitude less than the median value dominant probabilities in order to account for uncertainties in the data.

TABLE 1 PWR LARGE LOCA ACCIDENT SEQUENCES vs. RELEASE CATEGORIES

Core melt | No core melt

Release Categories								
1	2	3	4	5	6	7	8	9
Dominant Large LOCA Accident Sequences With Point Estimates								
AB-α $1x10^{-11}$ AF-α $1x10^{-10}$ ACD-α $5x10^{-11}$ AG-α $9x10^{-11}$	AB-γ $1x10^{-10}$ AHF-γ $2x10^{-11}$ AB-δ $4x10^{-11}$	AD-α $2x10^{-8}$ AH-α $1x10^{-8}$ AF-δ $1x10^{-8}$ AG-δ $9x10^{-9}$	ACD-β $1x10^{-11}$	AD-β $4x10^{-9}$ AH-β $3x10^{-9}$	AB-ε $1x10^{-9}$ ADF-ε $2x10^{-10}$ AHF-ε $1x10^{-10}$	AD-ε $2x10^{-6}$ AH-ε $1x10^{-6}$	A-β $2x10^{-7}$	A $1x10^{-4}$
Other Large LOCA Accident Sequences								
ACDGI-α AHFI-α ACHF-α ACDI-α ACDG-α AGI-α AFI-α ACG-α ACGI-α ACF-α ACDF-α ACEI-α ACEG-α ACEGI-α ACEF-α ACE-α AHF-α	ADF-β AHFI-δ ACHF-δ ACHF-γ ACDF-γ ACEF-γ AHFI-β ADFI-β ACHF-β ACDF-β AHF-δ AHFI-γ AEF-β AEFI-β ACEF-β AEF-δ AEFI-δ ACEF-δ AB-β AHF-β	AHG-α AHGI-α ADF-α ADFI-α ACH-α ACHI-α ACHG-α ACHGI-α AGI-δ AFI-δ ACG-δ ACGI-δ ACF-δ AHI-α ADGI-α ADI-α ADG-α AE-α AEI-α AEF-α AEFI-α AEG-α AEGI-α	ACDGI-β ADG- β ACDI-β ACDG-β ADGI- β ACE- β ACEI- β ACEG- β ACEGI-β AEG-β AEGI-β	AHI- β AHG- β AHGI-β ADI-β ACH-β ACHI-β ACHG-β AE- β AEI-β	ACHGI- ε AHFI- ε ADFI- ε ACDF- ε ACDGI-ε ACHF-ε AEF- ε AEFI-ε ACEF-ε ACEGI-ε	AHG-δ AHGI- δ AHGI- ε ACH-ε ACHI- ε ACHG- δ ACHG- ε ACHGI- ε ACDI- ε ACDG- δ ACDG- ε ADG- δ ADGI-δ AHG- ε ADI- ε ADG- ε ACD-ε ADGI-ε AHI-ε AE-ε AEI-ε ACE-ε ACEI-ε ACEG-ε ACEG-δ ACEGI-δ ACHGI-δ AEG-δ AEGI-δ AEG-ε AEGI-ε	AI-β AC-β ACI-β	AI AC ACI
$A\Sigma_p^{(a)}$	3×10^{-10}	2×10^{-10}	5×10^{-8}	1×10^{-11}	7×10^{-9}	1×10^{-9}	3×10^{-6}	2×10^{-7}	1×10^{-4}

(a) Σ_p is the arithmetic sum of the probabilities of the accident sequence in each release category.

probability discrimination technique has reduced the approximately 650 accident sequences to 78, or by roughly an order of magnitude.[1] Thus the use of the event trees and probability discrimination has reduced the total number of accident sequences of interest from about 130,000 to 78. To summarize, this reduction was accomplished by (1) the elimination of physically meaningless accident sequences (a reduction from 130,000 to 650) and (2) the elimination of low-probability accident sequences that have similar releases to those of much higher probability (a reduction from 650 to 78).

[1] See Table 2 which is Table 3-14 of Appendix V. The number of sequences (78) does not include sequences in which fuel melting does not occur.

Examination of these 78 sequences reveals that they have the general form that includes the frequency of occurrence of some initiating event (P_{IE}) times the probability of system failures (P_{SF1} x...x P_{SFn}) times the probability of one of the several possible containment failure modes (P_{CFM}). A detailed look at each of the 78 sequences shows that 48 of the sequences have the general form of P_{IE} x P_{SF} x P_{CFM} and 3 sequences involve single events.[1] Hence, 51 sequences involve the failure of only a single system or a single element; that is, at the system level, there can be no potential common mode failures in these sequences simply because there is only one system per sequence.[2] Potential common mode failures between systems and their components thus need be considered in only the remaining 27 sequences. Examination of Table 2 reveals that these 27 sequences involve only six different combinations of two-system failures; thus potential common mode combinations between systems had to be investigated in only six cases.[3]

The foregoing discussion leads to the extremely important conclusion that accident sequences that determine the probability of radioactive releases in reactor accidents are dominated by single-system failures. Furthermore, as will be discussed in section 4.2, the bulk of the predictions of system failure probabilities are also determined by single failures and single causes of failures within the individual systems. Thus it can be concluded that the probabilities predicted for reactor accidents are generally dominated by sequences having single-system failures and single causes of failures within systems.

As a final step in the assignment of values for the probability of occurrence of the various release categories in Table 2, it was necessary to take into account the uncertainties and variations in radioactive release magnitudes for the accident sequences. These variations are physical realities and can result from perturbations in the physical processes (temperatures, pressures, radioactivity removal efficiencies, etc.) involved in the accident sequences and in the precise timing of the various failures involved in the sequences. Such variations make it possible for a particular sequence to have some probability of being in more than one release category.

Since the values calculated for the radioactive release magnitudes for the sequences represented best estimates, it was necessary to assign a distribution of release magnitudes for each of the sequences in the various release categories. All accident sequences in a particular release category were assigned a 10% chance of being in the adjacent categories and 1% chance of being in the next adjacent categories. This in essence was a smoothing effect, which is discussed in greater detail in Appendix V, section 4.1.2.

The incorporation of smoothing affected both the consequences and the probabilities associated with accident sequences. For example, since smoothing permitted a particular sequence to have a 10% chance of occurring in the next highest release category, there are some cases (as can be seen from examination of Table 2), in which the probability of the occurrence of that larger release was essentially determined by this particular sequence and could be increased by as much as an order of magnitude. Figure 3 illustrates the net effect of the smoothing technique and shows that the probabilities of occurrence of several release categories were significantly increased.[4] It is interesting to note

---

[1] Of course the potential common mode failures among P_{IE}, P_{SF}, and P_{CFM} must be carefully studied. The potential common modes between P_{IE} and P_{SF} were studied as indicated in sections 5 and 6 of Appendix IV and as discussed in section 4.3 of this addendum. The combination of P_{IE} and P_{SF} can potentially result in core melt, thus causing a dependent containment failure; the resulting containment failure modes were extensively examined, as indicated in section 2.2 of Appendix I and in Appendix VIII.

[2] There are three single-event accident sequences in which system failures do not appear. These involve the check valve and reactor vessel rupture cases.

[3] The 27 sequences did not involve any combinations having more than two system failures per sequence.

[4] This figure is the same as Fig. V 4-1 of Appendix V.

TABLE 2 PWR DOMINANT ACCIDENT SEQUENCES vs. RELEASE CATEGORIES

	RELEASE CATEGORIES						Core Melt	No Core Melt	
	1	2	3	4	5	6	7	8	9
LARGE LOCA A	AB-α 1×10^{-11} AF-α 1×10^{-10} ACD-α 5×10^{-11} AG-α 9×10^{-11}	AB-γ 1×10^{-10} AB-δ 4×10^{-11} AHF-γ 2×10^{-11}	AD-α 2×10^{-8} AH-α 1×10^{-8} AF-δ 1×10^{-8} AG-δ 9×10^{-9}	ACD-β 1×10^{-11}	AD-β 4×10^{-9} AH-β 3×10^{-9}	AB-ε 1×10^{-9} AHF-ε 1×10^{-10} ADF-ε 2×10^{-10}	AD-ε 2×10^{-6} AH-ε 1×10^{-6}	A-β 2×10^{-7}	A 1×10^{-4}
A Probabilities	2×10^{-9}	1×10^{-8}	1×10^{-7}	1×10^{-8}	4×10^{-8}	3×10^{-7}	3×10^{-6}	1×10^{-5}	1×10^{-4}
SMALL LOCA S_1	S_1B-α 3×10^{-11} S_1CD-α 7×10^{-11} S_1F-α 3×10^{-10} S_1G-α 3×10^{-10}	S_1B-γ 4×10^{-10} S_1B-δ 1×10^{-10} S_1HF-γ 6×10^{-11}	S_1D-α 3×10^{-8} S_1H-α 3×10^{-8} S_1F-δ 3×10^{-8} S_1G-δ 3×10^{-8}	S_1CD-β 1×10^{-11}	S_1H-β 5×10^{-9} S_1D-β 6×10^{-9}	S_1DF-ε 3×10^{-10} S_1B-ε 2×10^{-9} S_1HF-ε 4×10^{-10}	S_1D-ε 3×10^{-6} S_1H-ε 3×10^{-6}	S_1-β 6×10^{-7}	S_1 3×10^{-4}
S_1 Probabilities	3×10^{-9}	2×10^{-8}	2×10^{-7}	3×10^{-8}	8×10^{-8}	6×10^{-7}	6×10^{-6}	3×10^{-5}	3×10^{-4}
SMALL LOCA S_2	S_2B-α 1×10^{-10} S_2F-α 1×10^{-9} S_2CD-α 2×10^{-10} S_2G-α 9×10^{-10} S_2C-α 2×10^{-8}	S_2B-γ 1×10^{-9} S_2HF-γ 2×10^{-10} S_2B-δ 4×10^{-10}	S_2D-α 9×10^{-8} S_2H-α 6×10^{-8} S_2F-δ 1×10^{-7} S_2C-δ 2×10^{-6} S_2G-δ 9×10^{-8}	S_2DG-β 1×10^{-12}	S_2D-β 2×10^{-8} S_2H-β 1×10^{-8}	S_2B-ε 8×10^{-9} S_2CD-ε 2×10^{-8} S_2HF-ε 1×10^{-9}	S_2D-ε 9×10^{-6} S_2H-ε 6×10^{-6}		
S_2 Probabilities	1×10^{-7}	3×10^{-7}	3×10^{-6}	3×10^{-7}	3×10^{-7}	2×10^{-6}	2×10^{-5}		
REACTOR VESSEL RUPTURE - R	RC-α 2×10^{-12}	RC-γ 3×10^{-11} RF-δ 1×10^{-11} RC-δ 1×10^{-12}	R-α 1×10^{-9}				R-ε 1×10^{-7}		
R Probabilities	2×10^{-11}	1×10^{-10}	1×10^{-9}	2×10^{-10}	1×10^{-9}	1×10^{-8}	1×10^{-7}		
INTERFACING SYSTEMS LOCA (CHECK VALVE) - V		V 4×10^{-6}							
V Probabilities	4×10^{-7}	4×10^{-6}	4×10^{-7}	4×10^{-8}					
TRANSIENT EVENT - T	TMLB'-α_8 3×10^{-8}	TMLB'-γ_7 7×10^{-7} TMLB'-δ 2×10^{-6}	TML-α 6×10^{-8} TKQ-α 3×10^{-8} TKMQ-α 1×10^{-8}		TML-β 3×10^{-10} TKQ-β 3×10^{-10}	TMLB'-ε_7 6×10^{-7}	TML-ε 6×10^{-6} TKQ-ε 3×10^{-6} TKMQ-ε 1×10^{-6}		
T Probabilities	3×10^{-7}	3×10^{-6}	4×10^{-7}	7×10^{-8}	2×10^{-7}	2×10^{-6}	1×10^{-5}		
(Σ) SUMMATION OF ALL ACCIDENT SEQUENCES PER RELEASE CATEGORY									
MEDIAN (50% VALUE)	9×10^{-7}	8×10^{-6}	4×10^{-6}	5×10^{-7}	7×10^{-7}	6×10^{-6}	4×10^{-5}	4×10^{-5}	4×10^{-4}
LOWER BOUND (5% VALUE)	9×10^{-8}	8×10^{-7}	6×10^{-7}	9×10^{-8}	2×10^{-7}	2×10^{-6}	1×10^{-5}	4×10^{-6}	4×10^{-5}
UPPER BOUND (95% VALUE)	9×10^{-6}	8×10^{-5}	4×10^{-5}	5×10^{-6}	4×10^{-6}	2×10^{-5}	2×10^{-4}	4×10^{-4}	4×10^{-3}

Note: The probabilities for each release category for each event tree and the Σ for all accident sequences are the median values of the dominant accident sequences summed by Monte Carlo simulation plus a 10% contribution from the adjacent release category probability.

that, with the use of smoothing, the cumulative probabilities for all core melt release categories shown in Table 2 are principally determined by only six sequences.[1] As stated in section 4.1.2 of Appendix V, the use of smoothing served to give greater confidence that potential common modes had been adequately treated and that any common modes not thought of would not likely affect the final release probabilities. In fact, the six sequences listed in footnote 1 involve only one double system failure (ML).

SUMMARY

The systematic and logical elimination of physically meaningless sequences and dependencies from the event tree that has been described in this section does much to lay to rest the typical "what if such-and-such were to happen?" questions that are generally encountered in the consideration of potential common mode failures. If the "what if" question does not fall within the accident sequences defined in the event tree, it is not a meaningful question and need not be considered further.[2] Thus the thought process that considers the potential interrelationships among the very large number of potential failures at the system and component levels and concludes that the number of potential common mode failures is so vast as to be unmanageable is, in fact, incorrect insofar as reactors of the type covered in this study are concerned. The discipline imposed by the event tree logic imparts the understanding that common

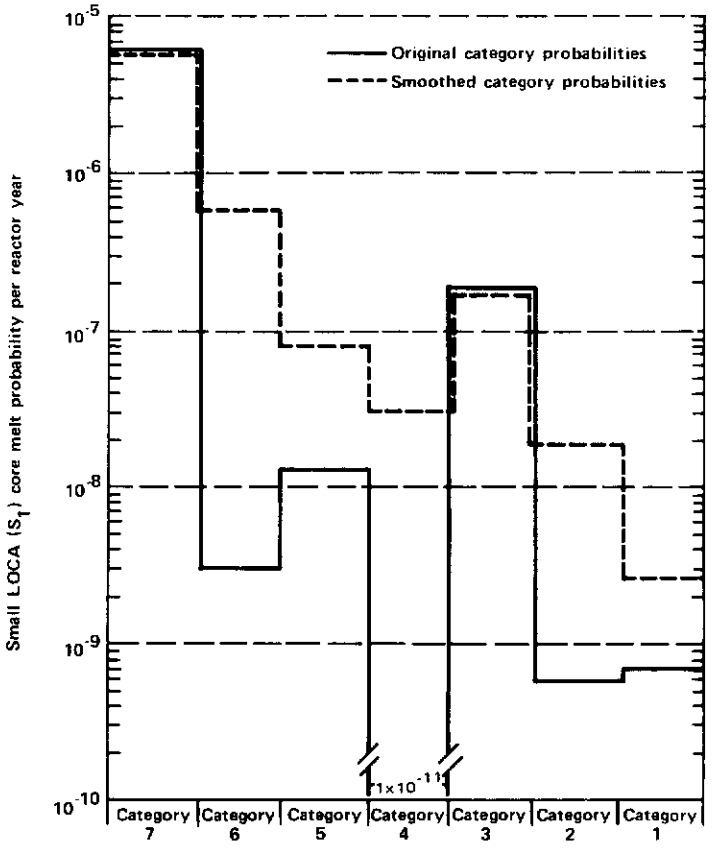


Figure 3 Application of Probability Smoothing

[1] S_2D-ε, S_2H-ε, S_2C-δ, V, TML-ε and TMLB'-δ.

[2] This only applies to failures originating within the plant; it does not apply to failures due to external forces or to acts of sabotage. These will be discussed in section 5.

mode failures between components in different systems are of no interest unless these components appear in systems involved in the same accident sequence and that common mode failures between systems are of no interest unless these systems are involved in the same accident sequence.

It is the view of the study that the development and use of event trees based on detailed knowledge of the nuclear power plants and of the engineering principles involved in the physical processes that could potentially occur in accident situations provided some of the principal insights gained in the performance of the overall risk assessment in WASH-1400.

4.2 FAULT TREE METHODOLOGY AND ITS CONTRIBUTIONS TO COMMON MODE FAILURE CONSIDERATIONS

As mentioned in the preceding section and as discussed in section 2.3 of Appendix I, the accident sequences defined by the event trees provide the fault tree analyst with the criteria for system failure as well as the context that describes the conditions under which the systems are required to perform. These criteria and contexts, which may vary for individual systems as they appear in different accident sequences in the event trees, are needed for the construction of fault trees in order to predict the proper probabilities of system failures that enter into the various event tree sequences in which they are involved. Whereas traditional fault tree approaches have often considered only single systems, the use of the event trees that define system interrelationships involving various combinations of system success and failure, varying definitions of system success and failure, control system interrelationships, etc., permits the fault trees to be constructed with greater attention to the applicability of the tree for its planned use and to the adequate treatment of potential common mode failures.

Once an event tree had been completed and the construction of fault trees started, common mode failures were incorporated into the fault trees and their quantification in six ways:

1. The fault trees were constructed to meet the criteria and context prescribed for the systems by the event trees; the fault trees were thus conditional fault trees.

2. The fault trees identified components that were common to multiple systems appearing in an accident sequence.

3. Each fault tree was developed to an extremely detailed component level in order to locate single component failures and potential common mode failures deep within the system.

4. Human failures were explicitly included in the fault trees, and dependencies between human failures were also included in the fault tree quantification.

5. Test and maintenance contributions were incorporated in the fault tree quantification along with dependencies involving test and maintenance.

6. Evaluations, including sensitivity and bounding studies, were performed to determine the possible impacts from common mode failures not previously considered in the earlier analyses.

The first five procedures listed above for handling common mode failures represent the major areas of the fault tree analyses performed in the study. Although these are the major ways in which it is thought that common mode failures can be identified, and although an intensive effort was made to define these areas as completely as possible, one cannot be certain that all significant common mode failures would be found by these procedures. The sixth area encompasses sensitivity and bounding studies that were performed to help check the completeness of the common mode coverage obtained by use of the earlier procedures. Each of the six procedures for handling common mode failures will be taken up in the discussion that follows.

1. Criteria and Context for Fault Trees

The first way the fault trees accounted for common modes was by incorporating the criteria for system failure and the environmental and timing contexts imposed on the systems by the event tree accident definitions. The criteria and context considerations are included in the component failure definitions in the fault tree and their subsequent quantification, which are made to be dependent on the accident sequence and accident conditions.

An example of the consideration of the criteria for system failure in specific accident sequences involved the defini-

tion of accumulator failure for the PWR emergency coolant injection (ECI) in the LOCA event tree. The accumulator portion of this system is so designed that two out of the three installed accumulators would have to fail to cause ECI failure in a particular sequence. In some specific LOCA situations, the rupture of the primary coolant system would negate the functioning of one accumulator, and therefore only one additional accumulator failure was required for system failure. For these specific situations, the fault trees analyzed the causes for only one accumulator failure.[1]

Another example that illustrates how potential dependencies due to accident environments can influence the analysis is found in the PWR containment spray recirculation system. Two of the pumps for this system were located inside the containment. In specific accident situations, the environment in the containment was of high stress (pressure, temperature, and radioactivity); the dependency of the failure of the pumps to the same adverse environment was incorporated by using pump failure rates applicable to such environments and by coupling the pump failure causes. In the general area of human failures, when actions were required to be performed quickly and the operators would be under stress due to accident conditions, higher probabilities of human failure were used.

The incorporation of such dependencies had a significant impact on the construction of the fault trees and in the assessment of component and human failure rates.[2]

2. Common Components in System Fault Trees

The second way the fault trees determined common modes, by identifying common components in multiple systems, is a standard output of the methodology. For each system failure in an accident sequence, a fault tree was constructed showing the components and basic events that could cause system failure. When the same component appeared in different systems, that component or event was given the same identification symbol to show the commonality.

To analyze an accident sequence, the fault trees of all the system failures in the sequence were combined ("anded" together) through the fault tree methodology. The Boolean analysis of the combined fault trees then extracted the common components and common events appearing in the different system fault trees, thus determining the single components and other single events that could cause more than one of the systems in the sequence to fail.

Since, as indicated earlier in section 4.1, the event trees were so effective in eliminating accident sequences involving multiple-system failures, there were only a limited number of remaining sequences where common components were identified. Table 3 lists 10 of the more significant accident sequences that involved multiple-system failures in which common components were identified.[3] Because of the large number of accident sequences that involved only single-system failures and because of the other contributions found in the fault trees, these common components in general had little effect on the predicted probability of accidents.

3. Detail in Fault Trees

The fault trees constructed in the study were developed to an extremely detailed level in an effort to ensure that significant common mode failures were incorporated in the trees. Each fault tree was constructed down to the basic component level to determine the basic causes of system failure; relays, wires, wire contacts, and gaskets are examples of the level to which the fault trees were developed. (Major components such as pumps, valves, diesels, etc., were of course also included.) A representative fault tree developed in the study consisted of roughly 300 basic component failure causes, 700 higher faults (intermediate between basic cause and system failure), 1000 fault relations (gates on the tree), and 30,000 combina-

---

[1] Section 5.6.2 of Appendix II contains a more detailed and thorough discussion of the accumulator modeling.

[2] The discussions accompanying each fault tree in Appendix II contain the actual detailed considerations used in the analysis and evaluation of each fault tree.

[3] A More complete discussion of this area is given in section 5 of Appendix IV.

TABLE 3 SIGNIFICANT ACCIDENT SEQUENCES INVOLVING COMMON-COMPONENT MULTIPLE-SYSTEM FAILURES

Sequence	Common-Component Failure
	PWR
ACDI	Storage tank failure[(a)]
SCDI	Storage tank failure[(a)]
AHF	Containment sump failure[(b)]
SHF	Containment sump failure[(b)]
ACF	Control system failure[(c)]
SCF	Control system failure[(c)]
	BWR
AE	Coolant injection (LPCIS) failure[(d)]
SE	Coolant injection (LPCIS) failure[(d)]
AI	Coolant recirculation (LPCRS) failure[(e)]
SI	Coolant recirculation (LPCRS) failure[(e)]

(a) These involve the refueling water storage tank. See Appendix II, sections 5.4 and 5.6.3.

(b) These involve the sump provided in the containment to collect water from the containment floor to make it available for continuous recirculation. See Appendix II, sections 5.7 and 5.9.

(c) These involve failures in the control system that initiates operation of the containment spray injection system and the containment spray recirculation system. See Appendix II, sections 5.4, 5.5, and 5.7.

(d) These include valve and pipe ruptures and failures in the central system for LPCIS. See Appendix II, volume III, section 6.4.2.

(e) These include loss of emergency service water and valve, pump, and pipe failures. See Appendix II, volume III, section 6.7.

tions of basic component failures that would result in system failure.

The extreme detail in the fault trees made it possible to identify single component failures and single human failures that would cause the entire system to fail. In addition, double failures and higher order combinations of failures were identified that had sufficiently high dependencies or sufficiently high failure probabilities such that, when combined, they acted like single failures in causing the system to have a high failure probability.

Because of the detail in the fault trees, it was possible to identify common causes and dependencies that were due not only to hardware but also to human and other causes. Examples include human calibration errors rendering multiple sensors to be failed in the consequence limiting control system and accident environments causing the operation of pumps inside containment to be dependent on the operation of containment spray recirculation system. These dependencies contributed to the system failure probabilities and helped to cause the higher system failure probabilities to be realized.

Some people hold the view that fault tree methodology will inherently predict probabilities of system failure that are much smaller than is achieved in practice. In some past work, system failure probabilities were often computed to be 10^{-8} to 10^{-9} and even lower. In contrast, Tables 4 and 5 present the distribution of unavailabilities associated with the systems analyzed in this study. As indicated in the tables, 77% of the PWR median system unavailabilities lay between 10^{-4} and 10^{-1}, showing the single-failure and high-probability contributions that were identified in the fault trees. If one considers the 95% upper bound, to account for data uncertainties, then 100% of the PWR system unavailabilities were greater than 10^{-4}. The relatively high unavailabilities predicted for most of the systems analyzed are due to single-component failures, single causes, and other single type failures.

These results are important with regard to common mode considerations. If the fault trees had not been developed in such detail, then the trees would have included, but would not have identified, failures that were dependent and that were caused by more basic single failures. In identifying the single-component failures, the basic causes were thus determined and the dependen-

cies resolved. A final point can be made about the relationship between the dominance of system failure probabilities by single failures and potential common modes not identified by the fault trees. Any common mode, at its utmost extreme, can change multiple failures to a single failure. From the data base in Appendix III, it is seen that the single-component and basic event probabilities (per demand) have values between 10^{-6} and 10^{-3}, with active components having the highest values.[1] Because the fault trees already have single failures and because of the high system probabilities already determined, there is not a great chance that additional common modes will impact on the results. There is thus reasonable confidence in the stability and insensitivity of the results obtained.

4. Human Error, Testing, and Maintenance Contributions

By including human errors and test and maintenance contributions in the fault trees and fault tree quantifications, common mode failures were covered in the fourth and fifth ways. Human failures were included in the fault trees and fault tree quantifications whenever the operator interfaced with a component or subsystem and could cause failure. Unavailabilities computed for components that were tested or maintained included failure contributions due to the downtime associated with these acts.

The inclusion of human failures and test and maintenance contributions was an important reason for the rather high values predicted for system failure probabilities (about 10^{-4} to 10^{-2}). Historically human failures and test and maintenance contributions were often not included in the fault trees and fault tree evaluations; this was particularly true when fault trees were constructed at the conceptual design stage of the system, where such information was generally not available.

From Appendix III it is seen that human failure probabilities can be quite high when compared to component failure probabilities. For example, in certain

TABLE 4 PWR CALCULATED SYSTEM UNAVAILABILITIES (22 SYSTEMS)

Median Unavailability Q_M	Number of Systems	Percentage of Systems in Each Unavailability Range	
$10^{-5} \leq Q_M < 10^{-4}$	5	23%	
$10^{-4} \leq Q_M < 10^{-3}$	4	18%	77%[a]
$10^{-3} \leq Q_M < 10^{-2}$	10	45%	
$10^{-2} \leq Q_M < 10^{-1}$	3	14%	

Upper Bound Unavailability Q_U	Number of Systems	Percentage of Systems in Each Unavailability Range	
$10^{-4} \leq Q_U < 10^{-3}$	7	32%	
$10^{-3} \leq Q_U < 10^{-2}$	7	32%	100%[a]
$10^{-2} \leq Q_U < 10^{-1}$	8	36%	

(a) Percentage of systems whose unavailability $\geq 10^{-4}$.

[1] Some systems had failure probabilities higher than 10^{-3} because they had human error or test and maintenance contributions, which will be discussed, or because they had a number of single-component failures.

TABLE 5 BWR CALCULATED SYSTEM UNAVAILABILITIES (18 SYSTEMS)

Median Unavailability Q_M	Number of Systems	Percentage of Systems in Each Unavailability Range	
$10^{-6} \leq Q_M < 10^{-5}$	1	6%	
$10^{-5} \leq Q_M < 10^{-4}$	4	22%	
$10^{-4} \leq Q_M < 10^{-3}$	7	39%	72%(a)
$10^{-3} \leq Q_M < 10^{-2}$	3	16.5%	
$10^{-2} \leq Q_M < 10^{-1}$	3	16.5%	

Upper Bound Unavailability Q_U	Number of Systems	Percentage of Systems in Each Unavailability Range	
$10^{-5} \leq Q_U < 10^{-4}$	2	11%	
$10^{-4} \leq Q_U < 10^{-3}$	7	39%	89%(a)
$10^{-3} \leq Q_U < 10^{-2}$	5	28%	
$10^{-2} \leq Q_U < 10^{-1}$	2	11%	
$10^{-1} \leq Q_U < 10^{0}$	2	11%	

(a) Percentage of systems whose unavailability $\geq 10^{-4}$.

circumstances there is a 10^{-2} probability that the operator will not open a manual valve.[1] This compares with a 10^{-4} probability that the valve will be closed due to inherent component failure or a 10^{-6} probability that the valve will be in a failed state due to rupture. (The probabilities are in units of "per demand.")

Test and maintenance contributions can likewise be relatively high when applicable. If a test or maintenance act requires 1 hour per week in which the component is rendered unavailable, then the test and/or maintenance contribution is 6×10^{-3} (which is obtained simply by dividing 1 hour by 168 hours in the week). This test and maintenance contribution is higher by a factor of 60 than a 10^{-4} component-related contribution and higher by a factor of 6000 than a rupture contribution.

Tables 6 and 7 give a breakdown of the various contributions that were calculated for the system failure probabilities categorized as to hardware, test and maintenance, human, and common mode, where common mode also includes human-caused dependencies.[2] As seen from the wide variation in the contributions from the given categories, it was important that all the various categories be considered in attempting to determine meaningful values for the system probabilities. The relatively complete coverage of all the category contributions gives a reasonable confidence that the modeling and calculations were properly performed and that common modes were adequately covered.

[1] The 10^{-2} probability applies to a single operator act with no monitoring or backup. The numbers quoted in this discussion are approximate general values, and the reader should refer to Appendix II for particular, applicable values.

[2] The contributions are based on the point value calculations given in Appendix II.

TABLE 6 CONTRIBUTIONS TO PWR SYSTEM UNAVAILABILITIES

System	Contribution (%)			
	Hardware	Test and Maintenance	Human Error	Common Modes[a]
Reactor protection	65	35		
Auxiliary feedwater:				
0-8 hours after small LOCA	5	9		86
8-24 hours after small LOCA	100			
0-8 hours without offsite power	<1	56		44
Containment spray injection	14	6		80
Consequence limiting control:				
Hi; single train	74	9	13	4
Hi; both trains	27	6		67
Hi-Hi; single train	61	26		13
Hi-Hi; both trains	6	2		92
Emergency coolant injection:				
Accumulators	59	41		
Low-pressure injection	16	23	60	1
High-pressure injection	80		19	1
Safety injection control:				
Single train	57	42		1
Both trains	13	19		68
Containment spray recirculation	7	56		37
Containment heat removal	86			14
Low-pressure recirculation	31	1	<1	68
High-pressure recirculation	25			75
Containment leakage	100			
Sodium hydroxide addition	3	77		20

(a) Includes human cause contributions.

5. Sensitivity Studies

In the sixth and final way of including common mode failures, evaluations and quantifications were performed that covered extraneous common modes and tested the sensitivity of the calculated system probabilities to additional common mode impacts. Appendix IV (sections 3 and 4 in particular) describes in detail the bounding (sensitivity) techniques and special engineering investigations involved in these common mode analyses.

With regard to the bounding and sensitivity analyses, whenever multiple component failures in the fault trees were judged to be susceptible to having common mode contributions that had not been previously identified, then a maximum impact was assigned for the possible common mode contribution. With this possible impact included, the system failure probability was then reevaluated to determine if any significant change occurred. When several susceptible combinations existed, all these combinations were assigned maximum impacts.

As described in Appendix IV, the maximum impact for common mode failures was assigned by allowing the combination of failures to become a single failure. The probability of failure for the combination thus becomes the probability for a single failure. With these single-failure probabilities used for

TABLE 7 CONTRIBUTIONS TO BWR SYSTEM UNAVAILABILITIES

System	Contribution (%) Hardware	Test and Maintenance	Human Error	Common Modes
Reactor protection	73	3		24[a]
Vapor suppression:				
Large LOCA	100			
Small LOCA	100			
Emergency coolant injection:				
Low-pressure coolant injection	17	83		
Core spray injection	8	92		
Autodepressurization	<1			100[a]
High-pressure coolant injection	15	85		
RCICS	14	86		
Containment leakage:				
Large LOCA				
Drywell (>6 $in.^2$)	2			98
Drywell (1-4 $in.^2$)	<1			100
Wetwell (>6 $in.^2$)	4			96
Wetwell (1-4 $in.^2$)	<1			100
Small LOCA	100			
High-pressure service water:				
Required within 30 minutes	3	44		53[a]
Required within 25 hours	10	43		47[a]
LPCRS and CSIS pump cooling (ESW)	100	<1		<1[a]
Secondary containment	100			

(a) Includes human cause contributions.

the combinations, the fault tree was then reevaluated to determine the change in the system failure probability.[1]

As given in Table IV 3-1 of Appendix IV, the common mode mechanisms examined in this sensitivity impact study were common mode failures due to (1) design defects; (2) fabrication, manufacturing, and quality control variations; (3) test, maintenance, and repair errors; (4) human errors; (5) environmental variations; (6) failures or degradation due to an initiating failure; and (7) external initiations of failure. In the bounding studies performed to check the validity of fault tree quantitative results, one technique used was to permit all components of the same generic type (e.g., all relays, all pumps, etc.) in a system to be interdependent. This analysis thus incorporated the types of common mode effects that could potentially be due to components having common manufacturers, common failure sensitivities, etc.

In addition to these sensitivity studies, which consisted essentially of mathematical analyses, special engineering investigations were performed on the accident sequences to determine any remaining possible common modes, including those due to external events and common component sensitivities.

These special engineering studies are also discussed in Appendix IV. These studies were concerned with common mode failures resulting in multiple systems failing in the same accident sequence.

[1]The single-failure probability was obtained from the minimum of the individual component probabilities in the combination, as indicated in section 3 of Appendix IV.

As described in sections 5 and 6 of Appendix IV, flywheel failures generating missiles, gas bottle explosions, vehicle crashes, and all motor valves failing due to manufacturing defects were among the detailed common mode causes examined. Components that have common properties and are potentially susceptible to common failure causes were investigated with particular care in these special engineering studies.

In general, the sensitivity studies and engineering investigations found no significant impacts from the common modes that were analyzed. This was due to the common mode analyses that had already been performed in the event trees and fault trees discussed earlier. The sensitivity studies and special engineering investigations thus tended to validate the thoroughness of the common mode analyses that had been performed and the insensitivity of the system and accident sequence probabilities to any further common mode contributions.

4.3 SUMMARY OF THE HANDLING OF COMMON MODE FAILURE[1]

The preceding sections have covered the individual contributions of event trees, fault trees, and data in the handling of common mode failures in the study. Additional perspective can be gained by considering the complete accident sequences needed to define overall risk to the public. The discussion, so far, has considered event trees that define the frequency of occurrence of some initiating event (P_{IE}) and the probabilities of various system failures ($P_{SF1} \times \ldots \times P_{SFn}$) that can potentially lead to core melting. There are additional factors that need to be considered in order to define complete accident sequences:

a. Core melt, per se, does not create a risk to the public because it occurs inside a containment building. For the radioactivity that is released from the molten fuel to be dispersed to the environment and expose people to radioactivity, the containment must fail. Appendix I, section 2, contains a detailed description of potential containment failure modes (P_{CFM}) given core melt. While it is virtually certain that core melt will cause a dependent failure of the containment, there are several modes in which the containment can potentially fail, each having a distinct probability and a distinct consequence.

b. Given the failure of the containment, the radioactivity will be dispersed to the environs of the reactor in a manner determined principally by the meteorological conditions existing at the time of the accident. The meteorological conditions are defined by such factors as atmospheric stability, wind speed, wind direction, etc. Since there is a probability distribution of weather conditions (P_{WC}) that may occur as a function of time, this distribution must also be considered as a part of an accident sequence.

c. Another factor that must also be considered is the probability distribution of population (P_{PD}) about reactors to take into account the probability that varying numbers of people may be exposed to the dispersed radioactivity.

As has already been discussed, in most cases the accident sequences involved situations in which the failure of a single system (following the initial failure) caused core melt. In a few cases, a single system failure combined with a single component failure is involved. There is also a wide variability in the frequency of initiating events as well as some variability in the failure probability of the various systems involved. Typical generalized sequences, covering the dominant contributions from the LOCA event tree and the transient event tree in the PWR, involve the following two illustrative formulations:

$$P_{IE} \times P_{SF} \times P_{CFM} \times P_{WC} \times P_{PD}$$

(for LOCAs) (1)

and

$$P_{IE} \times P_{SF} \times P_{CF} \times P_{CFM} \times P_{WC} \times P_{PD}$$

(for transients). (2)

---

[1] In this section, the symbol P represents probability and the various subscripts are defined as follows: IE = initiating event; SF = system failure; CFM = containment failure modes; WC = weather conditions; PD = population density; CF = component failure.

Such formulations are valid if the definitions of occurrence of the various events include consideration of the dependent failures among the elements. The discussion below is divided into two parts, one applicable to the LOCA event tree sequences and one applicable to the transient event tree sequences.

LOCA

In the case of the LOCA event tree, the initiating event is pipe rupture. The probability that it could cause failure of either the safety system or the containment was carefully examined, as indicated in Appendix IV, sections 5 and 6. No significant coupled failures of this type were found, presumably because specific design features are included in reactors to prevent such dependencies.

The combination of $P_{IE} \times P_{SF}$ produces core melt, which, as discussed earlier, will cause a dependent failure of the containment in one of a number of modes (P_{CFM}). Thus P_{CFM} is, in fact, a common mode failure probability that was carefully defined in Appendix VIII. The weather conditions and population density are essentially independent of one another and of the other factors in the equation.

It is interesting to note that formulation (1) yields, for the very large consequence values reported in this study, a probability of occurrence of approximately 10^{-9} per reactor-year. There are many people who have traditionally questioned the validity of predictions of low-probability events, and such questions must be regarded seriously because there have been many erroneously small predictions of system failure probabilities. Formulation (1), however, gives a different perspective of the probability prediction of 10^{-9}. For instance, in the case of the small-LOCA sequences in a PWR, the elements of this formulation have roughly the following values:

$$P_{IE} \simeq 10^{-3}$$
$$P_{SF} \simeq 10^{-2}$$
$$P_{CFM} \simeq 10^{-1}$$
$$P_{WC} \simeq 10^{-1}$$
$$P_{PD} \simeq \frac{10^{-2}}{10^{-9}}$$

The preceding discussion has already covered the principal common mode contribution, P_{CFM}, and indicated that there are no other significant common mode contributions. One might ask by how much these values might be in error. The value of P_{IE} is derived from pipe rupture data accumulated from many sources, as indicated in Appendix III, and is not likely to be very far in error. In fact, the only critical comments received from the public sector in this area suggest that the value used in the study is conservatively high and should be reduced to 10^{-4}.

The values of P_{WC} and P_{PD} are obtained from measured conditions in the real world and are known with greater precision than the other factors in the formulation.

The combined value of $P_{IE} \times P_{WC} \times P_{PD}$ is 10^{-6}. Thus the entire engineering (except for piping) of the plant, which includes the safety systems and the containment, accounts for a contribution of 10^{-3} ($P_{SF} \times P_{CFM}$) to the overall probability. In fact, the contribution of system unavailability (P_{SF}) is about 10^{-2}, and not in the range of 10^{-9} to 10^{-8} or less, as obtained in some early quantifications of system fault trees by others. Even if the values of system failure were grossly in error, the probability predicted for the largest accident would increase by a factor of only about 100.

TRANSIENT EVENT TREE

In the case of the transient event tree, the initiating event is the sum of the several types of transient events requiring rapid shutdown of the reactor. It is interesting to note that the frequency of occurrence of such events is approximately 10 per reactor-year, about 10^4 times more likely than the pipe rupture of 10^{-3} per year. On the other hand, the failure probability of the reactor protection systems (P_{SF}) is about 10^{-4} per demand and the failure of safety valves (P_{CF}) to reseat is about 10^{-2} per demand. The large consequence values reported in the study can be approximated generally as follows for transient events:

$$P_{IE} \simeq 10$$
$$P_{SF} \simeq 10^{-4}$$
$$P_{CF} \simeq 10^{-2}$$
$$P_{CFM} \simeq 10^{-1}$$
$$P_{WC} \simeq 10^{-1}$$
$$P_{PD} \simeq \frac{10^{-2}}{10^{-9}}$$

In examining the dependencies and the various factors among these elements, it is noted that there is some relationship between the 10 transients per year requiring shutdown and the probability of failure of the reactor protection system (RPS). Some of these transients involve the loss of offsite power, and the control rods are actuated to insert directly by the occurrence of this event; however, the failure probability of the RPS was not reduced because there is low coupling between this event and the principal causes of RPS failure. The transient event plus failure of RPS causes the reactor coolant system system relief valves to lift; the data determining the rate of failure of one of these valves to reclose includes potential dependencies involving this type of opening event. P_{CFM}, P_{WC}, and P_{PD} are as discussed earlier in connection with the LOCA event tree.

The total engineering contribution to the 10^{-9} probability in this case is $P_{SF} \times P_{CF} \approx 10^{-6}$. As noted earlier, P_{CF} comes from measured data, and only the P_{SF} value of 10^{-4} for the failure of the RPS is obtained from a fault tree. Using nuclear experience data of approximately 2000 demands of the reactor protection system, an approximate upper bound of 10^{-3} is obtained for the reactor trip unavailability.[1] From this actual experience, using the failure relationships as given in the sequence, the sequence probability can be in error by only about a factor of 10, yielding about 10^{-8} as an upper bound for the sequence probability.

To summarize the foregoing discussion, a number of probability factors must be combined in typical accident sequences to obtain the total risk probability, and the smallness of the risk probability comes from this process. System failure probabilities are only one element in the risk formulation, and potential common mode failures involving systems must be examined only in those factors that can affect the system failure probability. System failure probabilities obtained in the study were generally in the range of 10^{-4} to 10^{-2}, which is consistent with available experience and data. The sensitivity of the total risk probability derived from the formulations shown above can be bounded by using actual data or assuming the system probability to be unity. The limited variation in results when this is done shows the reasonableness of the study's methodology and final probability values.

---

[1] The upper bound estimate is obtained by using 200 reactor-years with approximately 10 demands of the trip system per reactor-year (i.e., monthly testing). Three failures are used for the upper 95% chi-square confidence bound.

Section 5

Completeness of the Consideration of Potential Accidents

WASH-1400 discussed the completeness of the coverage of potential accident sequences extensively in the following sections of the report: chapter 3, chapter 5 (section 5.4), and chapter 7 (section 7.1) of the Main Report and sections 2, 3, and 5 of Appendix I. The substance of these discussions is presented below.

The analysis of potentially large reactor accidents rests on the knowledge that the bulk of the radioactivity generated by the fission process will be retained in the uranium dioxide fuel pellets unless the fuel melts.[1] Fuel melting can occur only as a result of an imbalance between the heat being generated by the fuel and the heat being removed from the fuel. A heat imbalance can occur only as a result of LOCA or transient events. LOCA and transient events can potentially result from internal (random or coupled) plant failures, from external forces such as earthquakes and tornadoes, or from acts of sabotage. Many of these factors can potentially affect each of the various sources of radioactivity at the plant.

The places at which fuel is located in a nuclear power plant are the reactor core, the spent fuel pool, the refueling operation,[2] and the spent fuel shipping cask. By far the largest amount of radioactivity is located in the fuel in the reactor core since it contains both the largest accumulation of fuel and fuel that has had the least time for radioactivity to decay. The spent fuel pool, immediately after a refueling operation, has about 16% of the radioactivity of the core, and on the average has about 5%. The refueling operation, which handles only one fuel element at a time, involves about 0.3% of the core's radioactivity. The spent fuel shipping cask, having multiple fuel elements (~10) that have been subjected to a longer decay time, also contains about 0.3% of the core's radioactivity.

The much larger amount of radioactivity that resides in the core, as opposed to other locations, is only one of the reasons why the bulk of attention in the safety of nuclear power plants has been directed toward potential accidents involving only the core. Other factors are the potential for large releases of energy in core power transients and the potential for the release of the large amounts of stored energy in the reactor coolant system. These phenomena, as well as other processes that may be associated with them, not only might cause the fuel to melt, but also may provide a driving force to disperse the radioactivity released from the fuel. The potential for fuel melting and dispersal of radioactivity from the other fuel locations is significantly smaller.

In addition to examining all the places at which fuel is located at a nuclear power plant site, it is also necessary to examine the various forces that can act on the plant to cause release of the radioactivity from the fuel. Fortunately, the characteristics of uranium dioxide fuel are such that the bulk of the radioactivity generated by the fission process remains within the fuel pellets under normal conditions. The only way to release large amounts of radioactivity is to melt the fuel. Thus, a major factor in the safety of nuclear power plants rests on the prevention of fuel melting.

The two questions that must be examined are (1) whether the possibility even

---

[1] In addition to fuel, a nuclear power plant site has other potential sources of radioactivity (i.e., the waste gas and liquid waste storage tanks) that could be released as a result of accidents. However, these sources are very small (10^{-5} and 10^{-8} respectively of the core inventory) and do not have the potential to cause large consequences.

[2] During the refueling operation, a single fuel assembly is in transit between the reactor vessel and the spent fuel storage pool.

exists for the fuel in a particular location to melt, given the occurrence of potential accident conditions; and (2) what forces might act in such a way as to cause the fuel in a particular location to melt. The refueling operation and the shipping cask can be disposed of readily as candidates for contributors to overall risk, since it is hard to see how fuel can be made to melt in these situations. In the refueling operation, fuel elements cannot be lifted out of the water involved in the refueling process and, as long as the element is under water, it cannot melt. Furthermore, even if the one fuel element involved in the refueling operation could be exposed to air, calculations indicate that it would reach some equilibrium temperature (well below the melting point) at which it would be adequately cooled by the combination of heat radiation and convective air flow. In connection with potential shipping cask accidents,[1] calculations have shown that, even in the event of low-probability accidents that might break the cask and cause failure of the fuel cooling system, the fuel would not melt. Although some fuel cladding might be slightly damaged in such an accident, only very small amounts of radioactivity would be released to the environment. This radioactivity would be the small amount of the total fission gases produced that had migrated to the gap between the fuel and the cladding.

Based on the foregoing considerations, it appears that a potentially large release of radioactivity could only involve the fuel in the reactor core or in the spent fuel pool. The complete matrix of potential accidents must therefore cover the reactor core and the spent fuel pool as they might be affected by the various events that could potentially cause melting of the fuel. These events can be classed as internal (random or coupled) plant failures, external forces such as earthquakes and tornadoes, and acts of sabotage. These will be discussed in turn for each of the two locations of interest.

5.1 POTENTIAL ACCIDENTS INVOLVING THE REACTOR CORE

Figure 4 shows the matrix of potential accidents considered for the reactor core. Line 1 shows those accidents that

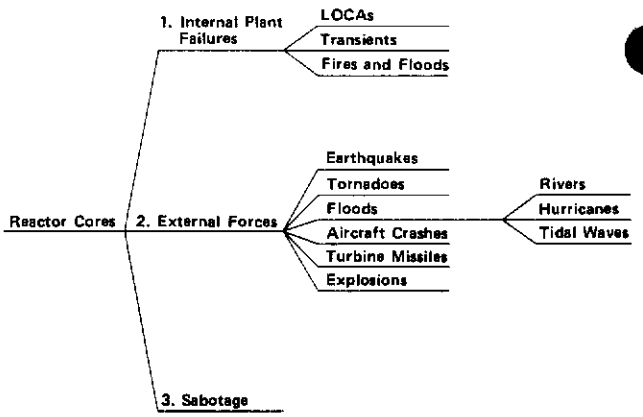


Figure 4 Coverage of Potential Accidents in Reactor Cores

can be initiated by internal plant failures. Line 2 shows those external forces that can potentially cause accidents of the type shown in lines 1a-1c. Line 3 shows the potential for accidents due to sabotage.

a. Figure 4, Line 1, Internal Plant Failures

The largest part of the Reactor Safety Study was devoted to the delineation of potential core accidents due to internal plant failures. The scope of this work is necessarily limited only to the consideration of imbalances between the heat being generated by the fuel and the heat being removed from the fuel because only such heat imbalances have the potential to cause the fuel to melt. Such imbalances can occur in only two ways: (1) as a result of transients in which the core power level exceeds the capacity of the heat removal systems to dissipate it or (2) as a result of LOCAs, in which the normal core cooling water is lost due to a rupture in the reactor coolant system and the core decay heat is not removed by the emergency core cooling systems. Sections 3 and 4 of this addendum and Appendices I through V describe in great detail the event tree/fault tree methodology used to investigate these classes of accidents. The total probability of core melt from these causes is predicted to be about 5×10^{-5} per reactor-year.

[1] WASH-1400 only examined potential shipping cask accidents that could occur at reactor sites. It did not consider transportation accidents.

It is also potentially possible for large electrical fires[1] originating within the plant to fail a sufficient number of systems within the plant to cause a transient or a LOCA that could cause the core to melt.[2] There is currently insufficient collected and collated data on the results of reactor and other industrial electrical fires to provide a generally applicable statistical basis for estimating the probability of core melt as a result of fires. However, analysis of the fairly recent fire at the Browns Ferry plant indicates that the likelihood of core melt due to such a fire would be about 1.0×10^{-5} per reactor-year and would represent about a 20% contribution to the overall likelihood of core melt.

b. Figure 4, Line 2, External Forces

It is necessary to consider whether the large forces that can be generated by some natural and man-made phenomena can cause any of the types of accidents developed in line 1 of Fig. 4 by causing the failure of the critical elements defined by the event tree/fault tree methodology. Thus it is necessary to examine both the likelihood of such external events and those portions of the plant that can be affected by the types of events shown on line 2 of Fig. 4.

The general approach[3] that has been taken in the design and location of nuclear power plants is to identify those elements of the plant whose continued operability is needed to ensure that the operation of the plant can be controlled, that the fuel in each location remains covered with water, and that the decay heat is removed from the fuel in each of its locations. Then the plant is required to be located and designed in such a way as to ensure that the likelihood of failures in these elements, due to each of the external forces, is quite small.

The study's handling of two of the external forces, aircraft impacts and turbine missiles, is easily illustrated. Since light planes cannot cause significant structural damage to a nuclear power plant, it is necessary to consider only the potential damage that can be caused by the larger aircraft. The probability of large aircraft crashes is well known, and thus it is relatively straightforward to compute the likelihood that a plane will crash at a site in such a way as to strike the plant. Taking into account the location of nuclear power plants with respect to airports (since this distance affects the likelihood of the crash) and the fact that not every such crash will cause an accident involving fuel melting, an overall probability of such an accident has been estimated to be 10^{-9} to 10^{-8} per reactor-year.[4] This value would not impact significantly on the predicted value of core melt of 5×10^{-5} per reactor-year.

Similarly, the probability of a turbine failure resulting in the generation of large missiles can be determined from an analysis of reported turbine failures. Taking into consideration the orientation of the turbine with regard to vital plant systems or components and the range of energies and trajectories associated with potential turbine missiles, the probability of striking a potentially vulnerable area can be calculated. The probability of penetrating structures and damaging critical equipment can then be calculated from the range of impact energies involved and the nature and thicknesses of protective barriers. As noted in section 5.4.5 of the Main Report, it has been estimated that the highest probability of a turbine missile penetrating the containment structure is 1.2×10^{-5} per reactor-year. Based on an examination of the physical layout of the plant, the chance of such a missile causing both a LOCA and the failure of sufficient safety systems to cause a

---

[1] Electrical fires refers to fires in which there is extensive enough burning of electrical cables to cause the inoperability of installed safety features. Burning may be initiated by electrical faults, current overloads, or external causes.

[2] See chapter 5 of the Main Report for a fuller discussion of large electrical fires. Sections 5 and 6 of Appendix IV discuss the potential effects of smaller fires.

[3] See USNRC Regulations 10CFR50, Appendix A, General Design Criteria for Nuclear Power Plants.

[4] See Appendix III, section 6.2, and Main Report, section 5.4.4, for a fuller discussion of this matter.

core melt appears to be negligibly small.

Certain plants may be exposed to other external hazards that are essentially unique to an individual site. Examples of these include sites adjacent to transportation routes that frequently carry munitions or other explosives or sites adjacent to chemical or petrochemical facilities, etc. Because such potential hazards are unique to specific sites, they have not been explicitly included in this study. Their inclusion was not considered necessary because only a relatively small number of plants are in locations where this type of consideration is necessary and because such plants are required to provide additional protection to reduce the probability of significant plant damage to a negligible value.

Similar analyses can be performed to analyze the effect of natural events such as floods, tornadoes, or earthquakes. The probability of occurrence of severe natural events can be calculated by the combination of generally limited historical data and analytical models. Based on a knowledge of the design parameters of the plant, the likelihood that a severe natural event could cause a core melt can then be estimated. These can be combined and compared with the likelihood of core melt determined by this study to determine if such events would have any impact on the risk from potential reactor accidents. As discussed in the Main Report, section 5.4, analyses of the external forces shown in line 2 of Fig. 4 indicate that external events are not expected to have a major impact on the risks associated with reactors.[1]

c. Figure 4, Line 3, Sabotage

The study concluded that, while there is no current methodology for comprehensively estimating the probability of successful acts of sabotage, any consequences produced by sabotage could not exceed the largest predicted by the study and would likely be much smaller. Section 5.4.6 of the Main Report discusses this matter in greater detail.

5.2 POTENTIAL ACCIDENTS INVOLVING THE SPENT FUEL POOL

Figure 5 shows the matrix of potential accidents considered for the spent fuel pool. As in Fig. 5, line 1 shows those accidents that can be initiated by internal plant failures, line 2 shows the external forces that can potentially cause accidents of the type shown in line 1, and line 3 shows the potential for accidents due to sabotage.

a. Figure 5, Line 1, Internal Plant Failures

Release of radioactivity from stored spent fuel can potentially result from heat imbalances causing melting of stored fuel or from mechanical damage to the fuel assemblies causing release of gap activity. Heat imbalances can result from loss of cooling water from the spent fuel storage pool; loss of the capacity to remove heat from the pool water, which would lead to boiling away of the pool water;[2] or an increase in

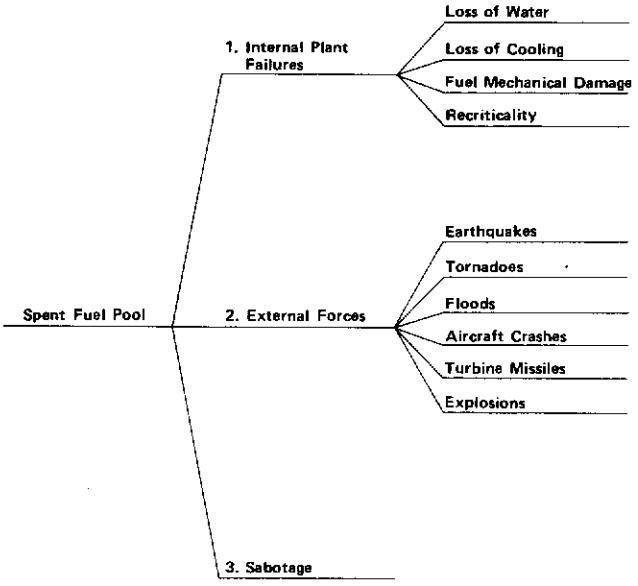


Figure 5 Coverage of Potential Accidents Involving the Spent Fuel Pool

[1] As indicated in chapter 7 of the Main Report, it would be useful to perform additional analyses in the future to determine whether the potential risks associated with external events can be estimated with greater precision.

[2] While it is indicated earlier in this section that a single fuel element in air will be adequately cooled, the large number of closely clustered elements in the fuel pool would prevent radiation of heat from the fuel from being an effective cooling mechanism.

the heat generation rate in the pool because the configuration of the fuel had been altered into a critical array, again leading to the boiloff of pool water. Section 5 of Appendix I discusses the bounding analyses that were performed to determine the potential risk associated with these accidents. As noted there, the potential releases are small in comparison to the releases associated with core melt, and the probability of occurrence is approximately two orders of magnitude below that associated with core melt.

b. Figure 5, Line 2, External Forces

As previously noted in section 5, it is necessary to consider whether the forces associated with external natural or man-made phenomena can cause any of the accidents developed in line 1. The probability of severe external forces at the plant is discussed in section 5. In general, that discussion is applicable to the stored spent fuel as well. In regard to external events, the design criteria of the spent fuel pool, the fuel building, and the pool cooling systems are similar to those used for systems that protect the core. Because of the very low probability of damage to stored spent fuel from random internal plant failures, external events are more likely to initiate an accident leading to release. The probability of failure in this manner is still quite low, however, and the potential releases, even assuming melting of the total inventory of stored fuel, are small compared to those associated with many of the reactor core accident sequences. This matter is discussed in greater detail in Appendix I, section 5.

c. Figure 5, Line 3, Sabotage

See section 5.1.c.

Section 6

The Handling of Failure Rate Data in Overall Risk Assessment

This section presents a summary of the data approach used in the study as well as its rationale. A more detailed discussion is contained in Appendix II, volume 1, and Appendix III, which have been rewritten to clarify the data treatment.

When the study initially tried to determine precise component failure rate values and other basic failure rate data (such as human failures) to use for the system and event tree quantifications, it found large uncertainties and large variabilities in the available data. These large variabilities existed not only for component data but also for human failure rates and initiating-event probabilities (e.g., pipe rupture rates). The nuclear reactor data that had been collected were neither sufficient nor detailed enough to yield accurate estimates of failure rates and basic event probabilities; furthermore, they showed a large variability from plant to plant. The other available industrial data showed similar variability in reported failure rate values, depending on the application and the reporting source.

Because of the large variability in the data, the study did not attempt to determine precise data values and precise probabilities, since these would have been meaningless. Instead, bounds were estimated for component and other data to determine the range in which data values could lie and hence give their variability. Because of the large spread, the failure rate data were treated as random variables, incorporating both the physical variability and the uncertainty associated with the data. Moreover, since the study's results were to apply to a population of approximately 100 nuclear plants, it was important to show the possible variability and uncertainty in this population.

For each failure rate, the study assessed an upper bound, which would give the pessimistic or worst case, and a lower bound, which would give the optimistic or best case. The range between the lower and upper bounds would then describe the variability that existed in the available data for the particular failure rate. The variabilities thus obtained for each failure rate were then propagated through the fault tree and event tree quantifications to give the corresponding variabilities for the system failure probabilities and accident sequence probabilities.[1]

To obtain a realistic representation of the ranges describing the possible failure rates, a wide variety of data sources were examined. To be applicable to the nuclear plant conditions that were to be quantified, the data sources examined had to be generally representative of industrial experience and industrial environments. However, certain Department of Defense data, obtained under controlled test conditions, and data representing more adverse environments encountered in certain plant applications were also included to give possible extreme values. The major sources of the data that were examined included the following:[2]

Edison Electric Institute (failure rate data)

Systems Reliability Service, United Kingdom

Failure Rate Data (FARADA) Handbooks published by the Fleet Missile Systems Analysis and Evaluation Group Annex

AVCO Corporation

Liquid Metal Engineering Center (nuclear data)

---

[1] In statistical terminology, the system probabilities were thus not strict probabilities but estimators.

[2] Appendix III gives a complete tabulation of the 77 sources used.

Holmes & Narver, Inc. (nuclear data)

The Chemical Engineer (Institute of Chemical Engineers, London, England)

Nuclear Safety Information Center, U.S. Atomic Energy Commission

Government-Industry Data Exchange Program (GIDEP) reports

Institut fuer Reaktor Sicherheit (Institute of Reactor Safety), West Germany

European nuclear agencies

Institute of Electrical and Electronic Engineers

Proceedings of RISO (Denmark) conferences

To serve as a final check on the ranges obtained from the various data sources, the limited data that were available from commercial nuclear power plant operation were analyzed separately and were compared to data obtained from other sources.[1] The final range assignments were found to be consistent with the commercial nuclear data.[2]

With regard to assuring that common mode failure considerations are adequately incorporated into the assessment, it is important to understand that the failure rate data examined cover many causally related failures, such as those due to manufacturing and construction defects, design errors, quality control inefficiencies, environmental conditions, as well as human and various other causes. Furthermore, it should be noted that both the general and the nuclear data included failures experienced in actual operation. Thus the failure rates used as the data base in the study, being principally derived from field experience, were essentially total failure rates, and not simply "random" failure rates (i.e., not failure rates due only to inherent, inexplicable component failure). Special common mode studies were thus needed to identify failure causes that were already included in the data.[3]

There were three exceptions to the foregoing: potential failure causes due to seismic loadings, tornado loadings, and the potential accident environments of high pressure, temperature, and radioactivity.[4] Certain nuclear components are required to remain operational under these conditions and are therefore designed to accommodate stresses of this type. Since neither nuclear nor nonnuclear components generally experience these stresses, their effects are not included in the data sources used to derive failure rate data for use in the study.

These considerations formed the basis of the design adequacy task described in Appendix X. Although NRC safety design requirements cover consideration of these stresses for applicable components, no experience data are available to test the validity of the implementation of these requirements because of the rarity of seismic and accident events. To ensure the adequate implementation of these "special" design requirements, a detailed examination of the design and testing of a selected number of components and systems was

---

[1] The nuclear data consisted of reports of failure occurring through 1973. Additional checks have recently been made of 1974 and 1975 data and showed no significant changes from the analysis reported in draft WASH-1400.

[2] In statistical terminology, the final assessed data ranges were found not to be inconsistent with the commercial nuclear experience. See sections 1, 2, and 3 of Appendix III for more detailed discussions of the actual analyses.

[3] The failure causes have an implied occurrence frequency in the data sources. If the occurrence frequency was assessed to be higher in the nuclear plant applications, then special analyses were performed. An example is the special adverse-environment pump failure rates determined in Appendix III. It was necessary to examine any multiple effects from a single cause, but the single-component failure rates could be used in the bounding techniques of Appendix IV to bound the common mode multiple effect.

[4] The impact of tornado loadings did not affect the results of the study significantly and are not discussed further here. See Appendix X for additional information.

made. The results of this examination indicated some deficiencies in these areas in that, while the designs were not inadequate, they appeared to have somewhat less design margin than might normally be expected. These results were used to make appropriate modifications to component failures in the fault tree and event tree quantifications and to estimate the probability of the failure of safety systems under seismic loads, as indicated in section 5.4.1 of the Main Report.

Using the data available from the various sources described earlier, a set of failure rate values was obtained for each component failure of interest (i.e., contained in the fault trees or event trees). This set was then used to construct a probability distribution that described the variability in the data.[1] With respect to the commercial nuclear data, the variability in component failure rate from plant to plant was in agreement (i.e., not inconsistent) with the obtained distribution.[2]

In applying the probability distribution approach, ranges covering 90% of the possible values were constructed for each failure rate. The upper bound was the 95th percentile of the distribution (such that the region between the bounds was 90%).

The log-normal distribution was used to obtain the specific range values for each failure rate. Section 3.6 of Appendix II describes the justification for using the log-normal distribution and the general insensitivity of the results to using this distribution. (A number of different distributions were tested, but no change in final system results was observed.) The ranges determined for each failure rate were generally one or two orders of magnitude in width. Within this variability, all the various data sources were therefore in agreement, and the range thus represented the resolution of the numbers that could be obtained.

To account for the possibility that the failure rates of some components could be high and others could be low, the failure rate distribution for each component was then propagated by Monte Carlo simulation to obtain the distribution of final system and accident sequence characteristics (e.g., system unavailabilities) that could be obtained from the different possible failure rate values of a component.[3] The 95th and 5th percentiles of the system or accident sequence distribution then gave the 90% range for the possible characteristics. These 90% final ranges thus represented the variability of the system and accident sequence results that was due to the variability in component data.

The above treatment of variability and uncertainty in the data represents only one of a possible number of ways of handling this problem; however, this treatment was found to be straightforward and generally applicable. Instead of estimating a precise value for a piece of data, the use of ranges was considered to be more realistic and more meaningful. This method was applied to human error data and initiating-event data as well as to component failure data. The data distributions were propagated to obtain the distribution and range on any final result, thus quantifying the associated variability and uncertainty.

---

[1] In essence, this is analogous to treating the data as a set of samples from a statistical population on which a statistical and probabilistic analysis can be performed.

[2] The above description of the probability distribution application is somewhat simplistic. For a more thorough discussion of the random-variable basis (and Bayesian implications), see section 3.6 of Appendix II.

[3] Section 3.6.2 of Appendix II describes the simulation procedures.

Section 7

Modeling Considerations for Event Trees and Fault Trees

The discussions that follow deal with some of the modeling concepts and considerations involved in the study's use of event trees and fault trees. This section discusses the basic logic and set-theory concepts of event trees and the use of fault trees in event tree models and presents an amplification of the basic ideas behind event tree modeling and the methods of using fault trees in conjunction with event trees.

a. Entries and States of an Event Tree

An event tree begins with a defined accident-initiating event. Different initiating events will produce different event trees, and the different initiating events must thus be cataloged and enumerated to obtain a defined set of accidents.

The enumeration of initiating events is obtained from basic physical considerations of the nuclear reactor power-generating process. For core melt accidents, for example, the initiating events are determined from the classification of the events associated with heat generation and removal. A more thorough discussion of the logic and physics involved in determining the initiating events defined in the study is given in Appendix I.

Once the initiating events are defined, the safety systems must be incorporated into the event tree structure. For a particular defined initiating event, all the safety systems that can be utilized after the accident are then defined and identified. Since a reactor has only a specified and limited number of safety systems, their definition and identification are straightforward. (Appendix I, section 2, discusses the system identification.) The safety systems that are identified are then structured in the form of headings for the event tree. This is shown in Example 1 for two safety systems that can be involved after the defined initiating event has occurred. (In this example, the safety systems are simply labeled "system 1" and "system 2.")

Initiating Event	System 1	System 2

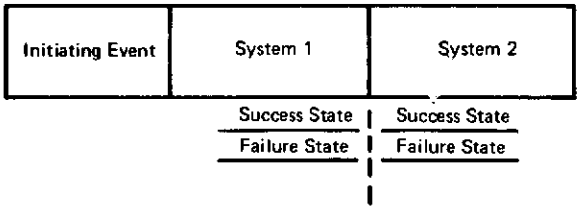
Example 1. Event Tree Heading

Instead of directly defining and identifying systems, which are associated with hardware, the event tree headings can be obtained by initially defining a set of functions to be performed by the safety systems. The functions relate to the physical processes associated with the system's operation, such as the function of heat removal. The set of functions acts as the initial heading of the event tree, and safety systems are then classified according to their relationship to these functions and subsequently substituted into the appropriate function heading. The result will again be a final heading consisting of the initiating event and the safety systems that can be involved. The study performed iterations involving event trees with both the hardware and functional headings to help check the adequacy of the modeling.

Once the systems for a given initiating event have been identified, the set of possible failure and success states for each system is defined and enumerated. Careful effort is required in defining success and failure states for the systems involved in the event tree to ensure that potential failure states are not included in the success definitions.[1] If dichotomous (two-state) modeling is employed, then one failed state and one success state is defined for each system; otherwise, a finite number of discrete states are defined (such as would be used when including partial failures).

Example 2 illustrates a two-state modeling for the systems of Example 1.

[1] In areas of uncertainty, potential success states that cannot be clearly demonstrated to be successful are assigned to the failure states.



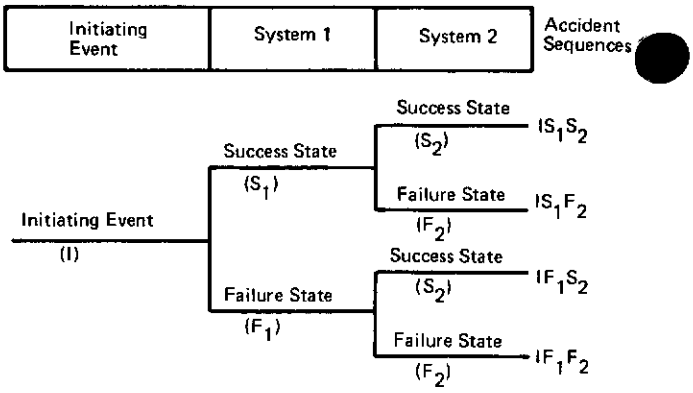
Example 2. System State Definitions for System 1 and System 2

Appendix I, section 2, discusses in some detail the definitions of system success and failure states used in the study as well as their rationale. Since the system state definitions constitute one of the most significant parts of event tree methodology, certain general points will be noted during the following discussion. With regard to these definitions, it is most important that the system failure and success states be defined within the context of the given initiating event and the other systems involved with the initiating event. Stated in a more probabilistic manner, the system failure and success states must be defined as conditional events. The context and conditionality will become more evident as the event tree methodology is carried through.

b. Event Tree Branching Logic

In carrying out the methodology, let us assume that the system failure states and success states have been properly defined, as shown in Example 2. The system states are then finally combined through the decision-tree branching logic to obtain the various accident sequences that are associated with the given initiating event. Tree branching simply involves connecting the states of one system to a particular state of another system. The branching is shown in Example 3 for the two-system illustration.

In Example 3, the initiating event is depicted by the initial horizontal line and the system states are then connected in a stepwise, branching fashion; system success and failure states have been denoted by S and F, respectively. The format illustrated follows the standard tree structure characteristic of decision tree methodology. The accident sequences that result from the tree structure are shown in the last column of Example 3. Each branch of the tree yields one particular accident sequence; for example, IS_1F_2 denotes the accident



Example 3 Illustration of Event Tree Branching

sequence in which the initiating event (I) occurs, system 1 is called upon and succeeds (S_1), and system 2 is called upon but fails (F_2) (i.e., system 2 is in a failed state such that it does not perform its defined function). For larger event trees, this stepwise branching would simply be continued.

c. Conditional Interpretation of an Event Tree

The event tree thus enumerates the possible accident sequences that are associated with the given initiating event and the systems that can be involved after the initiating event. Returning to the system state definitions, one sees that the system states on a given branch of the event tree must be defined and interpreted under the condition that the previous states in that branch have occurred; that is, the states are conditional on the previous states having already occurred.

As shown in Example 3, the success and failure of system 1 must thus be defined under the condition that the initiating event has occurred. In the upper branch of the tree corresponding to system 1 success, the success and failure of system 2 must therefore be defined under the conditions that the initiating event has occurred and system 1 has succeeded. In the lower branch corresponding to system 1 failure, the success and the failure of system 2 must be defined under the conditions that the initiating event has occurred and system 1 has failed. The conditional definitions in the event tree are the standard ones used in defining and modeling any combination (intersection) of occurring events.

Because of the conditionality interpretation, the event tree has great power in reducing the number of accident sequences that must be considered. For example, in the previous illustration, if the failure of system 1 caused system 2 to fail, or equivalently caused system 2 to be ineffective, then we would show no choices or alternatives for system 2 on the lower branch of the event tree, and this lower branch would simply be a straight, horizontal line containing only the failure of system 1. Instead of considering the accident sequences IF_1S_2 and IF_1F_2, we thus would consider only the sequence IF_1.

The identification of the conditional dependencies by the event tree methodology is important because, not only is the number of accident sequences logically reduced, but also system interdependencies are thereby incorporated and therefore need not be treated in later analyses. Whenever success or failure choices are not permitted for a system, the failure probability of that system is effectively being set equal to unity because of the previous events. (In the preceding example of removing the S_2 alternatives, the probabilities of the three-event sequences IF_1S_2 are not computed, but instead only the two-event sequence IF_1.) Appendix I has a detailed discussion of the identification of conditional dependencies that was done for the study's event trees because of system relationships. Because of this identification, many of the study's final accident sequences consisted of one or at most two system failures.

When timing and sequential considerations are important, the system state definitions must reflect them. For example, in the illustrated event tree, if there was a difference as to whether S_1 failed before or after S_2, then two event trees could be constructed where S_1 is the first failure and where S_2 is the first failure (i.e., effectively promoting the system headings). The study used dichotomous modeling in which one failure state and one success state was defined for each system. Care must be taken in these definitions in discretizing the failures and in incorporating partial failures. Appendix I discusses these considerations.

When the system states are detailed for their final definitions, then sufficient information exists to define the set of physical processes that will occur with each accident sequence. For example, for each sequence the study computed the magnitude of radioactivity release, which then served as a source term for the dose and risk calculations. In order to compute the radioactivity releases, it was necessary to incorporate the possible modes of containment failure in the event trees. This involved defining event tree headings that covered the possible failure modes that could occur (each failure mode effectively had two states: "occurring" and "not occurring"). The failure mode event trees were then combined with the system event trees to form accident sequences leading from the initiating events to the release of radioactivity from the containment.

d. The Use of Fault Trees

When the results associated with each accident sequence have been defined, the final task is to compute the probabilities of system failure. This is the place at which the fault trees enter. Generally, data on failures at the system level do not exist, and therefore the system failure probabilities must be estimated in terms of component failure rates, which are available. Thus, the system state definitions from the event tree can be used as defined "top events" of fault trees that are developed down to the component level. In the study, a fault tree was constructed for each defined system failure in the event trees. Because of the conditional definition of the system failures, the fault trees incorporated the conditionalities (i.e., previous events that have occurred) into their fault definitions and logic constructions. The quantitative system probabilities associated with the fault tree top events were system unavailability and system failure probability (failure to start and failure to run). Appendix II discusses the fault tree methodology and presents the fault trees that were constructed and used in the study.

A number of factors enter into the adequacy and power of a fault tree analysis, as it was used in the Reactor Safety Study:

a. The fault tree structure itself

b. The use of competent analysts having an intimate knowledge of the system and modeling process

c. The process of validating and rechecking the model and results

d. The examination of the results and probabilities to determine their sensitivity to possible omissions.

The fault tree serves as a logic structure in which the system is methodically and systematically analyzed to define those elements that contribute to its failure probability. A fault tree analysis is a deductive process in which a failure is traced back to its basic causes, including hardware and design causes, human error causes, and operational causes such as testing and maintenance. As the failure is being traced back, the fault tree logic structure organizes the steps that need to be taken and the items that need to be examined. One of the problems in a complex system analysis is the ordering problem: how to consider the various contributions in a systematic way so as to be thorough and comprehensive. The fault tree structure serves as the tool with which the analysis can be organized, blueprinted, and programmed.

Looking at past experience, the fault tree process was, in fact, developed and refined to deal with such complex situations. The Minute Man analysis and the analysis performed in the Space and Missile Organization (SAMSO) are examples of efforts in which fault trees were developed and utilized to handle the complex systems confronting the analyst. Even though it is certainly not foolproof, the fault tree process significantly reduces the chance of serious omissions in its systematic and methodical analysis procedure.

Though the fault tree structure serves to systematize the analysis, it does require a competent analyst to apply it in a competent manner. However, this is a requirement that applies to any field or endeavor (How many competent jobs are done by incompetent people?). The Reactor Safety Study tried to obtain the most competent people in employing the services of 12 skilled fault tree analysts. These fault tree analysts worked closely with the system to gain an intimate knowledge of its workings. Detailed system drawings, schematics, physical layouts, functional operating descriptions, and many on-site visits were involved in gaining the needed knowledge. The fault tree analysts also worked closely with experienced systems people who had a number of years of experience in reactor systems, reactor operation, and reactor safety. In addition, the fault tree analysts had the criteria and contexts derived from the event tree accident sequences to guide them in the construction of the fault trees.

To help further reduce errors, after the fault trees were constructed, they were checked and validated for their accuracy by identifying the dominant failure contributors. The fault trees were subjected to a standard evaluation process to determine not only the quantitative probability predictions but also the important qualitative system information. Such information includes, for example, the minimal cut sets, which in essence are listings of all the unique combinations of component failures that will cause system failure. This information was used in checking the logic, consistency, and accuracy of the fault tree.

In the Reactor Safety Study, to help ensure against omitting important contributors, large fault trees were constructed. For the accident sequences described in the event trees, a representative fault tree consisted of several thousand components and several thousand gates (logic structures). The evaluation process and the minimal cut sets were used to extract the dominant contributors to the system failure. Serving as an additional check, the minimal cut sets (i.e., component combinations) were then used to reconstruct "reduced fault trees," which helped to validate the accuracy of the larger trees with regard to dominant contributors. Furthermore, failure reports and incident reports filed with the AEC were examined for failures that had occurred in pertinent systems, and the larger fault trees were checked to ensure that they incorporated the types of failures that were occurring in operational systems.

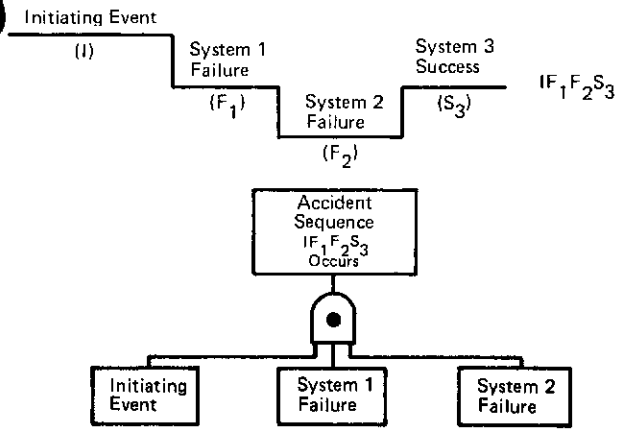
e. The Incorporation of Fault Trees into Event Trees

After the fault trees have been constructed by standard fault tree methodology, they are logically combined according to the accident sequences defined in the event trees. The logical combination effectively involves constructing a larger "accident sequence" fault tree from the individual system fault trees. The fault trees for the individual system failures in an accident sequence are combined through an intersection logic (an AND fault tree gate) to form the event of all the systems failing in the accident chain. Example 4 shows the associated fault tree construction for a given accident sequence composed of the initiating event (I), system 1 failure (F_1), system 2 failure (F_2), and system 3 success (S_3).

In Example 4, the symbol  denotes the fault tree AND gate; the event above the gate will occur if all the lower input events occur (an intersection relation). The boxes labeled "System 1 Failure" and "System 2 Failure" are to be replaced by the individual fault trees that have been drawn for these systems. In the example, the initiating event is also shown as an input event to complete the accident sequence definition.

"System 3 Success" is not shown in the illustrated accident sequence fault tree since it acts as an inhibiting, or restricting, condition (it could be shown by appropriate fault tree symbols). In the fault trees for systems 1 and 2, those shared components whose failure would also cause system 3 to fail are omitted since system 3 is given to have succeeded by the accident sequence definition.

If such system successes had been ignored in the study's fault trees of accident sequences, then a more conservative model would have resulted (yielding higher failure probabilities) since component failures could have been included that would have caused these successful systems to fail.



Example 4. An Accident Sequence and the Associated Fault Tree Construction

The accident sequence fault tree is thus simply a standard fault tree, and it can be evaluated and quantified using standard fault tree quantitative techniques. The component failures that are common to the systems are handled by standard, Boolean fault tree reduction techniques (e.g., any single failures that cause multiple systems to fail will be identified). The result of the quantitative evaluations will be the desired accident sequence probability that is to be associated with the accident results determined for that sequence. Appendix V describes the accident sequence manipulations and quantifications that were performed in the study.[1]

f. Output of the Event Tree and Fault Tree Evaluations

The preceding discussions described the event tree construction and quantification techniques used to obtain accident sequence probabilities. The event tree accident sequences also determined the physical processes and their timing involved in the various sequences. Separate analyses (described in Appendices V, VII, and VIII) determined the magnitude of radioactive releases for the various accident sequences. With a probability and radioactive release magnitude determined for each pertinent accident sequence, risk calculations can then be performed using these sets of values as source terms. The collection of probabilities and radioactive releases for the accident sequences in the various event trees gives the set of data points that serve as the basis for determining the risk from potential nuclear power plant accidents. The determination of the risk and the application of the accident sequence probabilities and associated radioactive releases are described in Appendix VI. The significant results of the overall risk analyses are presented in the Main Report.

[1] It should be noted that, instead of fault tree logic, any Boolean related logic could be used to combine the system failures in the accident chain. Also, the logic is applicable to multistate definition for the systems. The important factor is the identification of dependencies and the component failures common to the involved systems.

Section 8

Summary

The principal aspects of the methodology discussed herein pertain to the use of event trees, fault trees, and failure rate data to provide a systematic and logical framework for the definition and quantification of the probability and magnitude of radioactive releases in potential nuclear power plant accidents. While the use of this methodology is not new, its application in WASH-1400 has differences that are considered important:

a. The event trees used in this study differ significantly from the more conventionally used decision trees. In general, decision trees are the representations of a process whose adequacy depends principally on the skill and judgment of the analyst in properly conceptualizing the problem under consideration. While this type of skill applies to some degree in the event trees developed in WASH-1400, the analyst is aided very significantly because the elements of the trees are physical entities that exist in the nuclear power plant and the processes represented in the tree follow engineering and physical principles. The understanding of the details of plant design and of these physical principles assist the analyst greatly in ensuring a proper conceptualization for the reactor event trees.

b. The statistical treatment of variabilities associated with the inputs needed in the quantification of system fault trees and event tree accident sequences is an important new step. The treatment of these input data as random variables thus included their associated variability and uncertainty, and this enabled the study to use a broad base of applicable reactor and industrial hardware failure data as well as data associated with human errors, testing, and maintenance.

c. The sensitivity studies performed in connection with the quantification of system fault trees to test for the effects of unidentified potential common mode failures were also important in that, among other things, they permitted all components of the same generic type (e.g., all relays, all pumps, all valves, etc.) to be interdependent.

d. The understanding that common mode failures can be effectively handled as a matter amenable to engineering principles backed up by bounding statistical analyses represents a significant step forward in the quantitative application of event tree and fault tree methodology.

The event trees used in the study performed a powerful filtering function by providing a framework that (1) defined sets of potential accident sequences that were in essence complete for the initiating events involved and (2) provided logical methods based on knowledge of plant design and engineering principles to eliminate physically meaningless sequences from the otherwise complete event trees. Although the event trees used in the analysis of the PWR encompassed approximately 130,000 potential accident sequences, which could have conceivably involved millions of potential common mode failures at the system level, elimination of physically meaningless dependencies reduced the number of sequences of physical significance to approximately 650. The use of probability discrimination techniques among accident sequences that would produce similar radioactive releases reduced the number of potentially significant sequences from 650 to 78. Fifty-one of these sequences involve the failure of only a single system or a single element. In the 27 remaining sequences, only seven different combinations of two-system failures were involved. Therefore, of the potential millions of system-to-system common mode failures involved in the initially defined 130,000 potential accident sequences, only seven potential dependencies remained. Thus the event trees provided the basis for making the definition of potential common mode failures amenable to realistic analysis.

The systematic and logical elimination of physically meaningless sequences and dependencies from the event trees does much to lay to rest the typical "what if such-and-such were to happen?" questions that are generally encountered in the consideration of potential common mode failures. If the "what if" question

does not fall within the accident sequences defined in the event tree, it is not a meaningful question and need not be considered further. Thus the thought process that considers the potential interrelationships among the very large number of potential failures at the system and component levels and concludes that the number of potential common mode failures is so vast as to be unmanageable is, in fact, incorrect insofar as reactors of the type covered in this study are concerned. The discipline imposed by the event tree logic imparts the understanding that common mode failures between components in different systems are of no interest unless these components appear in systems involved in the same accident sequence and that common mode failures between systems are of no interest unless these systems are involved in the same accident sequence.

It is the view of the study group that the development and use of event trees based on detailed knowledge of the nuclear power plants and of the engineering principles involved in the physical processes that could potentially occur in accident situations provided some of the principal insights gained in the performance of the overall risk assessment in WASH-1400.

Several procedures were followed in developing fault trees that were specifically directed toward the identification of potential common mode failures. These included the construction of the trees to meet the criteria and contexts prescribed by the event trees, the identification of components common to multiple systems, the development of the trees to a detailed level to locate single and common mode failures, and the inclusion of human error as well as testing and maintenance contributions. Finally sensitivity studies were performed to bound potential common mode contributions; these caused little change in the fault tree quantifications. As indicated earlier, a significant contributor to this success was the treatment of data as random variables and the propagation of their associated variabilities throughout the fault tree and accident sequence quantifications. Finally, in the two cases where the probability of failure of systems could be obtained from field data, it confirmed the a priori predictions derived from the system fault trees.

In regard to the ability to successfully quantify low-probability events, the accident sequences derived from the event trees, when the effects of weather and population distributions are considered, can be generally characterized as follows:[1]

$$P = P_{IE} \times P_{SF} \times P_{CFM} \times P_{WC} \times P_{PD},$$

that is,

$$10^{-9} = 10^{-3} \times 10^{-2} \times 10^{-1} \times 10^{-1} \times 10^{-2},$$

where P_{IE}, P_{WC}, and P_{PD} are derived from measured data and where the only potential common mode that exists between $P_{IE} \times P_{SF}$ and P_{CFM} has been defined. Thus, the total engineering contribution to the overall probability of the largest consequences reported in the study amounts to 10^{-3} for the combined failure probability of a safety system and the containment.

---

[1]The symbol P represents probability and the various subscripts are defined as follows: IE = initiating event; SF = system failure; CFM = containment failure modes; WC = weather conditions; PD = population density; CF = component failure.

References

1. A. E. Green and A. J. Bourne, Reliability Technology, Wiley-Interscience, London, 1972.

Attachments

Attachment 1: NASA Letter

Attachment 2: Letter from Mr. A. E. Green

Attachment 3: GAO Report

Attachment 1

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
WASHINGTON, D.C. 20546

OFFICE OF THE ADMINISTRATOR

JUN 16 1975

Honorable William A. Anders
Chairman
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Dear Bill:

In accordance with your request, we brought together a group of Reliability and Safety Management people from both Headquarters and from the Johnson Space Center to discuss the Rasmussen Report on Reactor Safety with members of your staff. Comparisons were made of techniques used, data bases available, reliability prediction accuracies versus actual experience, etc. The discussion produced a set of comments with which NASA concurs and which we hope will be of value to you in the preparation of your final draft of the Reactor Safety Study. These comments are as follows:

1. The fault tree and event tree methodology used in the Reactor Safety Study is an effective technique and is similar to safety analysis methodology NASA has used.

2. This methodology is capable of producing numerical assessments of value in making design decisions if the data base from which probability of failures is determined has sufficient accuracy and content.

3. NASA has not been using the numerical assessment portion of the methodology because our data base is of small size. This is due to the lack of repetitive missions and changing hardware configurations. It has always been the NASA policy to pursue hardware failures until the precise failure mechanism is fully understood and to take immediate corrective action to prevent failure recurrence. This corrective action has created significant configuration differences from shot to shot even within the small family of

vehicles which might be considered repetitive--hence, the small data base from which to draw failure probability information.

4. NASA is not in a position to validate the numerical assessments in the Rasmussen Study because of the extensive efforts such a validation process would require.

5. NASA recommends that the NRC use the output of the study for more than just risk assessment. The identified systems engineering alternatives can be useful in making trade-off studies on design and operational improvements and these could be of value.

I understand that further discussions are planned with Quality Control personnel from both our staffs to exchange experiences in the inspection area. Please call on us for any further assistance we might provide.

Sincerely,

George M Low for

James C. Fletcher
Administrator

Attachment 2

SYSTEMS RELIABILITY SERVICE
A service to industry operated by the United Kingdom Atomic Energy Authority.

Our ref: SRS/POL/5/2
Your ref: AEG/27

Please reply to: Culcheth

Headquarters:
UKAEA, Wigshaw Lane, Culcheth,
Warrington, Lancashire, WA3 4NE.
Warrington 31244, Ext.
Telegrams: ATEN Warrington Telex: 62301

Harwell Section:
B521, AERE, Harwell Didcot, Berkshire.
Abingdon 4141, Ext.

Mr Saul Levine
Project Staff Director
Reactor Safety Study
Nuclear Regulatory Commission
Washington DC 20555

28 April 1975

Dear Saul

When I visited Washington DC in January, we had a short discussion on the correlation between predicted reliability characteristics and field experience.

As you are aware we have been associated particularly with land based plant equipment and systems involving electronics, electrical and mechanical items but excluding structures. We have found that where we have applied quantatitive reliability techniques of prediction, for example, for the failure rate of equipment then there has been reasonable agreement with field experience when it has become known. In the majority of the cases of this type which we have studied the agreement between the predicted and practical failure rates has been within a factor of two to one. It has also been our experience that in assessing the reliability of systems for safety purposes it has not always been necessary to have precise reliability data to decide whether or not the system is adequate.

As you know the Systems Reliability Service concerns itself with applying quantified reliability techniques in cooperation with its Associate Members. For your information, I enclose in Appendix I a current list of these Associate Members. A typical list of the areas in which reliability assessments have been carried out is also enclosed in Appendix II.

The results of the application of these techniques have been most encouraging and there is a continuing and expanding demand for this type of quantified assessment. In addition such assessments are very useful in contributing to certain aspects of decision making and for injecting discipline into design analysis. For your information I give in Appendix III a list of a few references which cover some of the aspects which I discussed with you.

Initially you may like to look at Pages 541 to 553 of reference 7 for some overall discussion. For some 50 system elements which we studied, the ratio of observed failure rate to predicted failure was between 0.26 and 2.6 (Figure 13.4). The other references of which I enclose copies should give you a little more specific information.

Needless to say in the development of any technology such as reliability technology we are continuously developing and investigating the methods and I would be interested to have your comments.

Yours sincerely

Eric

A E Green
General Manager
National Centre of Systems Reliability

Attachment 2 (Continued)

SYSTEMS RELIABILITY SERVICE

A service to industry operated by the United Kingdom Atomic Energy Authority

ASSOCIATE MEMBERS

As at April 1975

Danish Atomic Energy Commission
Reactor Division, Oak Ridge National Laboratory, USA
Central Electricity Generating Board
Security and Control Division of CNEN, Italy
Civil Aviation Authority
Imperial Chemical Industries Limited
Fast Reactor Design Division of CNEN, Italy
Junta de Energia Nuclear, Spain
Atomic Energy Board, South Africa
Commission des Communautes Europeennes, Belgium
AE & CI Limited, South Africa
Department de Surete Nucleaire, Centre d'Etudes Nucleaires de Saclay, France
DRAM Project, Norway
British Gas Corporation, Newcastle upon Tyne
Forsvarets Teletekniska Laboratorium, Sweden
MOD(N)
Technical Research Centre, Finland (TRCF)
South of Scotland Electricity Board
European Space Research Organisation
Motor Columbus, Switzerland
United States Atomic Energy Commission
Centec - West Germany
Shell International, The Hague
British Petroleum Company Ltd.
Laporte Industries Limited
NIRA, Genoa, Italy
Pilkington Bros. Ltd.
Nuclear Installations Inspectorate of Department of Energy
British Nuclear Fuels Ltd.
The Mining Research and Development Establishment of The National Coal Board
PPG Industries Inc., USA
A.M.N. (Ansaldo Mechanico Nucleari), Genoa.
Nypro (UK) Limited.
C.A. Parsons & Co.Ltd.
Instituto Elettrotecnico Nazionale Galileo Ferraris, Turin, Italy

Appendix II

Nuclear reactors

High pressure die casting machines

Criticality monitoring and alarm systems

Normal and standby electrical supply and distribution systems

Chemical plant automatic protective systems

High pressure relief and protective systems

Electronic and electro-mechanical logic sequence circuits and systems

Hazardous gas alarm systems

Medical engineering equipment

Plant measurement and control systems

Cooling water systems and their associated controls

Investigations of repair and maintenance characteristics

Actuator systems

Fire detection and control systems

Emergency electrical generating systems

Marine engine control systems

Chemical plant hazard evaluations

Plant availability studies

Boiler feed systems and sequence control systems

Electronic and control equipment evaluations.

APPENDIX III

1. EAMES, A. R. "Reliability Assessment of Protective Systems", Nuclear Engineering, March 1966.

2. GREEN, A. E. "Reliability Prediction", Institute of Mechanical Engineers, 1969.

3. BOURNE, A. J. "General Results of an Investigation into the Reliability of High Pressure Die Casting Machines", S.R.S Generic Report No. SRS/GR/5.

4. GREEN, A. E. "A Review of System Reliability Assessment", S.R.S Generic Report No. SRS/GR/20.

5. BOURNE, A. J. "Reliability Assessment of Technological Systems", Institution of Electrical Engineers, 19th October, 1971.

6. EAMES, A. R. "Principles of Reliability for Nuclear Reactor Control and Instrumentation Systems", U.K.A.E.A. Report No. SRD R1, September 1971.

7. GREEN, A. E & BOURNE, A. J. 'Reliability Technology', Published by John Wiley & Sons, 1972.

COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-164105

The Honorable Mike Gravel
United States Senate

Dear Senator Gravel:

This is in reply to the letter of July 31, 1974, signed by you and Senators Proxmire, Clark, Hart, and Brooke, asking us to compare reliability predictions for defense and space programs with actual performance and to provide some guidance on the value of reliability predictions. Your request was based on concern over how much confidence could be placed on reliability predictions for nuclear power reactors, particularly the possibility of catastrophic accidents.

We studied Department of Defense (DOD) and National Aeronautics and Space Administration (NASA) documents and other literature relating to reliability predictions, experience, and estimating methodology. We also interviewed experts, both within and outside the Government, to ascertain their views on this subject. From this limited study we conclude that:

1. Although the basic reliability methodology is adaptable to Atomic Energy Commission (AEC) projects, DOD and NASA experience has limited usefulness in judging the validity of AEC's reliability predictions.

2. The confidence that can be placed on reliability predictions is directly related to the extent of previous testing or use of the same or similar systems.

3. Most early DOD reliability predictions are goals set for the contractors or laboratories to achieve in development and production. Most such goals are not initially achieved in operations; but equipment and component modifications, training, and experience usually result in upward reliability trends over a period of time.

4. Reliability of major new systems cannot be accurately predicted because of the many variables--materials, training, maintenance, and so forth--that are involved.

Outlined below are the data we developed on reliability predictions, actual reliability, and specific systems performance.

RELIABILITY PREDICTION

Reliability experts are reluctant to make absolute predictions at the outset of new systems, mainly because so many variables are as yet unknown or unquantifiable. On the other hand, if the configuration is one of a well-understood series or similar to other tried configurations, test and experience data can often be extrapolated with some confidence. NASA and DOD interviewees believe that thorough testing in the intended operational environment and extensive experience data are the best guides to predicting reliability. Predictions are made during development, but these are used for comparison only--to choose among design alternatives, candidate components, and so on.

During development, reliability engineers use predictive models based on component testing. To anticipate the frequency of rare occurrences, tens of thousands of components must be analyzed to establish failure rates and to try to uncover some of the "unknown unknowns" that beset complex designs. This procedure can be costly and time consuming without producing all the answers about how a system will perform. Even though failure rates may be established through exhaustive testing, they are often modified by engineering judgment. For example, a manufacturer's stress ceiling on a critical component might be halved to temper the uncertainty of a reliability calculation.

Because of the uncertainties and inherent limitations in their ability to predict reliabilty, most engineers believe that an expressed level of reliability should be a goal rather than a confident prediction of how a new system will perform. Reliability goals, in their view, are guides for analyzing designs, selecting and testing critical components, providing for redundancies, choosing backup parts, and deciding on failure-avoidance measures.

Some officials look on contract-specified reliability figures as optimistic possibilities rather than supportable figures. One official termed contract-specified reliability numbers as "window dressing." Another expert said that accurate predictions may be unpopular or politically unacceptable. A recent Air Force report states that:

> "* * * where a manufacturer is interested in having his equipment look good he can, and will, select some of the more optimistic data he can find or generate, to use in his reliability predictions. Thus reliability predictions, for several reasons, tend to be generally optimistic by a factor of two to six, but sometimes for substantially greater factors."

ACTUAL RELIABILITY

Actual reliability in operations is affected by many variables. For example, changes in humidity, temperature, vibration, and shock cause problems in electronic systems. Human error, "wear-out," shipping, handling, and various maintenance practices are other causes of system failure. (NASA found that an intensive "people motivation" program improved overall reliability.)

Many problems are due to design "unknowns" not predictable or quantifiable during development. For example, one NASA official told us that six redundant components had failed on one system. If such a contingency could have been anticipated, the design would have been changed or further redundancy or backup parts added.

Reporting of actual reliability data is sometimes inadequate so that predictions versus achieved performance for systems and subsystems can be misleading. A recent Defense Advance Research Projects Agency report stated about defense systems:

> "There is no routine field-reliability reporting system in DOD that can provide meaningful feedback to producer commands and to manufacturers on the field reliability of electronic subsystems. Existing maintenance data collection systems * * * do not perform this function adequately. Moreover, there is considerable confusion in the terms used to describe reliability * * *. Thus field information is ambiguous at best."

NASA, on the other hand, with its "one shot" systems gets quick notice of failures, although the causes may not be readily ascertainable.

MAJOR SYSTEMS RELIABILITY DATA

The information on reliability of various defense and space systems shown below was developed by DOD, NASA, and other sources. We did not verify their accuracy, nor did we attempt to define what was meant by system reliability in each case. The data, therefore, is useful only for comparing initial estimates with later experience--system by system.

Selected Acquisition Reports (SARs)

These documents are published periodically by DOD to report technical schedules and cost information on certain major weapon systems. Nomenclature in the SARs varies; for example, the criteria for missile system performance are variously "system reliability," "in-flight reliability," "preflight reliability," "developmental prototype reliability," or "production prototype reliability." They are seldom defined. Combat reliability, which is usually a fraction of laboratory or test range levels, is not shown.

Electronic subsystems

Electronic subsystems apparently present the most reliability problems. A recent Defense Science Board report presented the following data on the specified versus actual mean time between failures (MTBF) (hours) of aircraft radar subsystems.

Aircraft	Specified MTBF (note a)	Achieved MTBF (note a)
F-4B	10	4
A-6A	75	8
F-4C	10	9
F-111 A/E	140	35
F-4D	10	10
A-7 A/B	90	30
A-7 D/E	250	12
F-4E	18	10
F-111D	193	less than 1
F-4J	20	5

a/ Approximate figures.

NASA systems

NASA experts believe that "absolute" reliability numbers are misleading and that the time required to develop them is better spent on critical-component reliability analyses. It does make predictions during development to compare design alternatives and to evaluate components. NASA's reliability experience to 1974 can best be illustrated by its history of launch successes, which average about 85 percent. Only in small samplings, it will be noted, is 100-percent reliability achieved.

B-164105

NASA Launch Vehicle Performance

Vehicle	Total	Successes	Success percentage
Mercury Blue Scout	1	0	0
Juno II	10	4	40
Jupiter C	1	0	0
Thor-Able	5	3	60
Vanguard	4	1	25
Atlas-Able	3	0	0
Atlas	11	9	82
Thor	2	2	100
Little Joe	7	7	100
Little Joe II	5	4	80
Scout X	1	0	0
Scout	57	51	89
Redstone	5	5	100
Thor-Delta	99	90	91
Thor-Agena	13	12	92
Atlas-Agena	26	20	77
Atlas-Centauer	32	26	81
Saturn I	10	10	100
Titan II	12	12	100
Atlas X-259	2	2	100
Gemini (Atlas-Agena Target)	6	4	67
Saturn IB	8	8	100
Saturn V	13	12	92
Total	333	282	85

As far as we could learn during this brief review, DOD and NASA officials can offer little guidance as to how very rare failures or catastrophic accidents to systems can be anticipated, avoided, or predicted. Failure rates for most engineered systems cover a very wide range. According to several reliability experts, simple mechanisms (ordnance fuzes) or systems liable to incur human losses have failure rates of 1 in 1,000 to 1 in 100,000 occurrences.

NASA goes to extraordinary lengths--reliability cost is hardly an object--to prevent disasters in manned space vehicles and has the singular advantage of vehicle occupants prepared to make onboard repairs. Still, three astronauts were lost in one vehicle. The Soviets suffered similar losses

in other attempts. No one can tell if and when such catastrophic failures will be repeated.

If you have any further questions on these matters, we shall be glad to discuss them with you and your staff.

Sincerely yours,

Elmer B. Staats

Comptroller General
of the United States