WASH—1400—App-11
(NUREG-75/014—App-11)

Reactor Safety Study

An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants

Appendix XI

United States Nuclear Regulatory Commission

October 1975

DISCLAIMER

WASH–1400
(NUREG 75/014)

ANALYSIS of COMMENTS
on the
DRAFT WASH - 1400 REPORT

APPENDIX XI
to
REACTOR SAFETY STUDY

U.S. NUCLEAR REGULATORY COMMISSION
OCTOBER 1975

Appendix XI

Table of Contents

Table of Contents (Continued)

List of Tables

List of Figures

Section I

Introduction

With the release of WASH-1400 in draft form in August 1974, the Reactor Safety Study requested comments from a broad spectrum of society. Comments were requested from environmental groups, groups critical of nuclear power, lawyers representing environmental groups and industry, government agencies, and industrial organizations representing reactor manufacturers, architect engineering firms and electric utilities. About 90 organizations and individuals responded with comments totaling about 1800 pages; these included many unsolicited comments.[1]

The comments received were in the main constructive and of considerable assistance in preparing the revisions to the draft report. This appendix provides a discussion of the principal comments received and guidance as to the location and substance of the significant changes incorporated into the final report. The large majority of comments grouped conveniently into 16 major topics, each of which is discussed in a separate section of this appendix, as indicated by the following list:

Section 2. Summaries of Principal Comments by Various Organizations

- 2.1 U.S. Environmental Protection Agency
- 2.2 American Physical Society Study Group on Reactor Safety
- 2.3 U.S. Atomic Energy Commission Regulatory Staff
- 2.4 Advisory Committee on Reactor Safeguards
- 2.5 Union of Concerned Scientists
- 2.6 Resources for the Future, Inc.

Section 3. Methodology

Section 4. Consequences Model

Section 5. Probability of Accident Sequences

Section 6. Radioactive Releases from Accident Sequences

Section 7. Emergency Cooling Functionability

Section 8. Reactor Vessel Rupture

Section 9. Nuclear Excursions

Section 10. Behavior of Radionuclides in Soil and Water

Section 11. Core Meltdown Analysis

Section 12. Steam Explosion

Section 13. Hydrogen Combustion

Section 14. Data Base

Section 15. External Forces

Section 16. Sabotage

Section 17. Scope

Section 18. Design Adequacy

Section 19. Miscellaneous

To handle the large volume of comments received in a coherent manner, it is necessary to present the essence of the comments and the appropriate responses. The action taken in response to the various comments received was based on an examination of each comment, both individually and in terms of the context provided by the comments from all sources. Many of the comments received from the various sources were similar and were therefore grouped to make their treatment easier to follow; the sources of the comments that were grouped together are identified in each case. For

[1] The organizations and individuals that submitted comments are listed in Table XI 1-1. Those whose comments were requested by the Study Group are indicated by asterisks.

further clarity, a discussion of the principal comments received from organizations that made a significant effort to review draft WASH-1400 is also presented.

Some of the comments received required changes to be made in the report. Most of these comments pertained to the calculation of consequences; in response, an essentially entirely new Appendix VI, Calculation of Reactor Accident Consequences, has been incorporated into the final report. Responses to those other comments that required changes in the report are also included in this appendix, with a notation indicating where the report has been changed. A second, somewhat larger, category included comments that addressed matters of significance and seemed to require a response to clarify the matter; it was felt that these comments did not require changes in the report.

The rest of the comments, comprising the large majority of those received, were of a nature that did not affect the study significantly and required no response. Many of these contained helpful suggestions that were essentially editorial in nature, and minor changes were made in the text of the report where appropriate. The comments in this category fell into the following subcategories:

a. The comment received was keyed to a particular section of the report and indicated that some sort of information or analysis was missing. The information sought was already contained elsewhere in draft WASH-1400, but apparently could not be found by the reader because of the large volume of the report. (It should be noted that where this type of comment identified areas of significance that were not covered in the report, the matter is discussed in this appendix as a part of the major topics listed earlier.)

b. The comment suggested expanding the scope of the study beyond that defined by its charter or extending the detail of the work beyond that needed to substantiate the point involved. Most comments of this type are not discussed in this appendix. However, a representative group on the scope of the study was assembled and is discussed in section 17.

c. The comment appeared to result from misreading or misunderstanding the report, or was in error.

d. The comment disagreed with material in the report without presenting factual information or analysis to substantiate the objection.

e. Minor editorial comments that were made to improve clarity, comprehensiveness, or consistency (or simply to correct fairly obvious errors); appropriate changes were made in the report where indicated. Some editorial comments made no such contributions or reflected merely matters of taste and were not acted upon. The report was not affected in any substantive way by comments of this type.

All of the substantive comments that were received are discussed in the various sections of this appendix. The principal areas addressed by these comments were the methodology used in the study, the calculations of consequences, and the probabilities and radioactive release magnitudes predicted for the various potential accidents. A reexamination of these areas led to the following actions by the study:

1. Because the discussions of methodology were scattered throughout the rather voluminous appendices and because certain elements that could have provided a better perspective of the methodology were not included in the draft report, an overview of the methodology was prepared. This overall discussion of the methodology is contained in section 3 of this appendix and in Addendum I to the Main Report. It is hoped that this overview will clarify the application of the methodology in WASH-1400.

2. In general, the potential consequences predicted in the final report have increased over those predicted in the draft report. All predicted consequences in the final report, except one, were within the factors of 1/3 and 3 error bands of the values predicted in the draft report. The predicted average value of latent cancers increased by a factor of about 7, due principally to the error made in the weathering half life that was assigned for cesium decay in the draft report. This effect also increased the land area needing decontamination by 5 and that in which relocation is required by 10. Early illnesses were calculated on an organ by organ basis which increased the magnitude by a factor of 6. The rest of the changes were within the confidence bounds of the predictions in the draft report. The study believes that its current consequence model is conserva-

tive and that the potential consequences in the final report represent near upper bound limits for those consequences such as early effects, property damage and contaminated land areas. This area is discussed further in section 4 of this appendix and in Chapter 5 of the Main Report. The above noted changes do not change the basic conclusion of the draft report that reactor risks are relatively small compared to other societal risks.

3. Although the probabilities predicted for the various accident sequences have changed in some details, the overall predicted probability of accidents did not change significantly. A number of changes affecting accident sequences, their probabilities, and radioactive release magnitudes are discussed below.

a. One accident sequence was identified that, although it had been considered qualitatively in the analysis, had not been treated quantitatively in the draft report. This sequence pertained to the potential contribution to risk of large electrical fires such as the one that occurred at the Browns Ferry Nuclear Power Plant. Section 3, comment 3.2.1 contains an analysis of this sequence, and the Main Report has been modified appropriately. The addition of this sequence did not have a significant impact on the results of the study.

b. In regard to the probabilities predicted for various accident sequences, the predicted probability for one sequence was changed as a result of the comments received. This involved the predicted probability for loss of ability to stop the fission process in certain BWR accident sequences. Although the probability of these sequences increased by a factor of 3, the net impact on the overall probability of accidents did not change significantly. See the response to comment 5.1.1 in section 5 of this appendix.

c. As the result of a comment questioning the applicability of the release magnitudes computed for large-LOCA accident sequences to small-LOCA and transient accident sequences, the study reexamined this area and performed additional computations of the potential radioactive releases from small-LOCA and transient accident sequences. These computations generally confirmed the study's engineering judgment in the draft report except for one transient sequence in the BWR. This change affects BWR release category 2. The releases of the halogens and alkaline earths, which are the principal contributors to the consequences of potential accidents, increased by 50 and 67%, respectively. The releases of strontium and tellurium also increased by factors of 2.5 and 3, respectively. These changes have been incorporated into Appendix V, section 1, and into the input to the consequence model described in Appendix VI. See response to comment 6.1 in section 6 of this appendix.

d. It should also be noted that in the preparation of the final report the study reexamined the probability predicted for each significant accident sequence as well as the assignment of radioactive release magnitudes for these sequences. Some minor errors were found both in the predicted probabilities of various accident sequences as well as in the predicted release magnitudes. When these were adjusted, the overall probability of core melt of 6×10^{-5} per reactor-year predicted in the draft report decreased slightly to 5×10^{-5} per reactor-year. In addition, some small increases and decreases in predicted radioactive release magnitudes also occurred. These changes as well as those mentioned in paragraph c. above (see sections 5 and 6 of this appendix for a more detailed discussion) produced no significant changes in the results of the study.

As indicated above, the principal comments received are covered in the following sections of this appendix:

Section 3. Methodology

Section 4. Consequence Model

Section 5. Probability of Accident Sequences

Section 6. Radioactive Releases from Accident Sequences

In addition, section 2 of this appendix contains brief summaries of the principal comments received from the U.S. Environmental Protection Agency, The American Physical Society Study Group on Reactor Safety, the U.S. Atomic Energy Commission Regulatory Staff, the Advisory Committee on Reactor Safeguards, the Union of Concerned Scientists, and Resources for the Future, Inc. These organizations apparently made significant efforts to evaluate the study and were responsible for a substantial portion of the substantive comments received. The summaries in section 2 are included to provide a basis for understanding the flavor and thrust of both the comments and the study's response to them.

TABLE XI 1-1

ORGANIZATIONS AND INDIVIDUALS SUBMITTING COMMENTS ON DRAFT WASH-1400[a]

Governmental Organizations

1. Brookhaven National Laboratory*
2. East Tennessee Development District
3. Federal Energy Administration*
4. Federal Power Commission*
5. Lawrence Livermore Laboratory
6. Minnesota Pollution Control Agency
7. National Aeronautics and Space Administration
8. Nuclear and Thermal Energy Council, State of Oregon
9. U.S. Atomic Energy Commission, Division of Reactor Research and Development*
10. U.S. Atomic Energy Commission, Director of Regulation*
11. U.S. Atomic Energy Commission, Advisory Committee on Reactor Safeguards*
12. U.S. Atomic Energy Commission, Office of Planning and Analysis*
13. U.S. Atomic Energy Commission, Regulatory Staff*
14. U.S. Department of Commerce
15. U.S. Department of Health, Education and Welfare*
16. U.S. Department of Interior
17. U.S. Environmental Protection Agency*

Nongovernmental Organizations

18. Aerojet Nuclear Company
19. American Physical Society Study Group on Reactor Safety
20. Atomic Industrial Forum
21. Babcock & Wilcox*
22. Bechtel Power Corporation*
23. Businessmen for the Public Interest*
24. Californians for Safe Nuclear Energy
25. Combustion Engineering, Inc.*
26. Concerned Californians
27. Edison Electric Institute*
28. Electric Power Research Institute*
29. Engineering Decision Analysis Company
30. Fluor Pioneer, Inc.*
31. Franklin Institute
32. Friends of the Earth*
33. General Atomic Company*
34. General Electric Company*
35. Gibbs and Hill, Inc.*
36. Gilbert Associates, Inc.*
37. Holmes & Narver, Inc.*
38. Institute for Energy Analysis
39. Iowa Student Public Interest Research Group
40. Medical Research Council
41. Natural Resources Defense Council, Inc.*
42. National Rural Electric Cooperative Association*
43. Nuclear Energy Liability Property Insurance Association
44. Nuclear Fuel Services
45. Philadelphia Electric Company
46. Pollution and Environmental Problems, Inc.
47. Public Interest Research Group
48. Rensselaer Polytechnic Institute
49. Resources for the Future, Inc.*
50. Sargent & Lundy Engineers*
51. Scientists' Institute for Public Information*
52. The Detroit Edison Company
53. The National Intervenors*
54. Town of Enfield Safety Council
55. Union of Concerned Scientists and the Sierra Club*
56. United Engineers & Constructors, Inc.*
57. University of Washington, Nuclear Physics Laboratory
58. Virginia Electric Power Company
59. Westinghouse Electric Corporation*

60. Wildlife Research Center
61. York Committee for a Safe Environment

Individuals

62. Louis Baker, Argonne National Laboratory
63. S. K. Ballal, Tennessee Technological University
64. Robert E. Barrett
65. Burton G. Bennett
66. Russell M. Bimber
67. Mrs. Elva I. Bresler
68. H. D. Bruner
69. William M. Bryan
70. Lincoln Clark, Jr., Massachusetts Institute of Technology Research Reactor
71. G. E. Cummings, Lawrence Livermore Laboratory
72. William Dooly, U.S. Atomic Energy Commission*
73. D. E. Dorfan
74. J. E. Falletta, Jr.
75. John D. Furber, Jr., University of California
76. Donald P. Geesaman
77. Richard L. Grossman
78. R. Keller
79. Jerome Kohl, North Carolina State University at Raleigh
80. Ralph Lapp*
81. Skip Latimer
82. Amory Lovins
83. Robert D. Millberry
84. R. F. Taschek, University of California - Los Alamos
85. Bill Teague
86. Richard E. Webb
87. Mrs. Mary Wright

(a) An asterisk indicates that the comment was solicited by the Reactor Safety Study. It should be mentioned that a number of other organizations whose comments were solicited did not respond.

Section 2

Summaries of Principal Comments by Various Organizations

This section presents the principal comments received from the U.S. Environmental Protection Agency, the American Physical Society Study Group on Reactor Safety, the U.S. Atomic Energy Commission Regulatory Staff, the Advisory Committee on Reactor Safeguards, the Union of Concerned Scientists, and Resources for the Future, Inc. These organizations apparently made significant efforts to evaluate the study and were responsible for a substantial portion of the substantive comments received.

2.1 U.S. ENVIRONMENTAL PROTECTION AGENCY

The U.S. Environmental Protection Agency's (EPA) comments on draft WASH-1400 were received on December 4, 1974, and August 20, 1975.[1] Where appropriate, the report was amended to reflect the changes recommended by the EPA. The comments received were a significant aid in preparing the final report.

The principal comments submitted by the EPA are presented below and are accompanied by responses where appropriate.

COMMENT 1

"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, and 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 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."

COMMENT 2

"There are a number of areas of nuclear power technology which should be considered as candidate areas for future application of a refined form of the Reactor Safety Study methodology, including different versions of contemporary light water reactors, high temperature gas cooled reactors, liquid metal fast breeder reactors, and variations such as barge mounted power plants."

RESPONSE

The areas mentioned here are outside the scope of the Reactor Safety Study, as indicated in section 17 of this appendix. The study agrees that it would be useful to pursue the areas outlined in future NRC work.

COMMENT 3

"The [EPA] second phase review findings indicate that although errors, omissions and other deficiencies were found in areas of draft WASH-1400, the vast majority of these were found not to have a significant effect on the overall risk estimates. More than a dozen areas were investigated in this phase but the only one which was found to have a significant potential for increasing the esti-

[1] The EPA letter of August 20, 1975, also forwarded a report entitled A Review of the Draft Report Reactor Safety Study (WASH-1400) by Intermountain Technologies, Inc. (ITI). ITI performed as a contractor to assist EPA in the review of WASH-1400.

mate of overall risks was the assessment of transient-without-scram accidents for boiling water reactors...."

. . . .

"Draft WASH-1400 shows that the transient-without-scram accident sequences for boiling water reactors (BWRs) make a major contribution to the overall accident risk. The treatment of several aspects of transient-without-scram accidents should be carried out in more detail to avoid unrealistically high risk estimates; an example is the determination of the combinations of control rods whose failure results in failure to scram. Other aspects of transient-without-scram accidents need better justification of the failure probability values chosen; the assessments of the single control rod insertion failure rate, of the multiple and common mode control rod insertion failure rate, and of the protection provided by the liquid poison injection system are such that higher failure probability values could have been selected from the information given, with a potential for increasing overall risks by as much as a factor of 2."

RESPONSE

The EPA comment that the probability contribution to BWR risk from transients without scram was under-estimated in the draft WASH-1400 report is generally correct. Each of the points made in the comment concerning the assessment of 1) single control rod failure rate, 2) the multiple and common mode control rod insertion failure rate and 3) the protection provided by the liquid poison injection system have been discussed in comment 5.1 of section 5 of this appendix. These discussions can be summarized as follows:

a. The single control rod unavailability of 10^{-4} per demand used in WASH-1400 is consistent with available data. See comment 5.1.3 in section 5 of this appendix.

b. Because of the nature of common mode failure contributions, the probability of multiple rods failing to scram does not vary appreciably as the number (>3) of potential rod failures increases. See comment 5.1.4 of section 5 of this appendix.

c. The estimated probability of 3×10^{-2} assigned in the draft report for failure of the operation to start the liquid poison injection system was in error. A better value of 10^{-1} has been assigned and as the final report has been changed accordingly. See the introduction to section 5 and comment 5.1.1 for a fuller discussion of the area.

COMMENT 4

"Although the draft Reactor Safety Study report does not make an absolute judgment on nuclear power plant accident risk acceptability, the comparative risk approach presented in the summmary and in the main volume of the draft report is likely to imply an acceptability judgment to the average reader. EPA recognizes that the comparative risk approach is a first step in addressing this question, but by itself is misleading. The summary presentations in draft WASH-1400 serve to illustrate some of the problems with the comparative risk approach, as do some of the observations on the subject in ITI's report. It is not an accurate comparison to compare risks estimated from calculations to risks estimated from experience, to omit latent deaths from comparisons of fatalities nor to compare acute fatalities to latent. A better appreciation of the risk estimates could be gained if their uncertainties were added to the graphs. It should also be acknowledged that the risk from nuclear power is not only the risk from severe accidents, but it also includes the risks from normal operation of nuclear power plants, from associated transportation and storage of radioactive material, from other fuel cycle facilities, and from such potential activities as sabotage and terrorist diversion of materials. It should be made clear in the final WASH-1400 that the study attempts to quantify the risk of accidents from contemporary light-water reactors and does not, by itself, make judgments on the acceptability of quantifications made, although such quantifications may be put into perspective through appropriate comparison with other risks.

"Our major reservation with respect to this study is the implied acceptability of the estimated risks to society. Although the study has made major inroads into quantification of accidental risks from nuclear reactors, the acceptability to society of such accidental risks has not been analyzed. It appears that WASH-1400 cannot, nor should it, address the acceptability to society of the risk estimates derived. It is important, however, that WASH-1400 not be susceptible to the interpretation that it presumes such acceptability. Thus, the quantification of risk determined by this study and implications of their

acceptability should be clearly differentiated to eliminate any potential confusion. The Reactor Safety Study's summary presentation should be modified to qualify the risk comparisons with more emphasis that they are only a first step toward the evaluation of risk acceptability and that conclusions with regard to the acceptability of the risks can only be drawn when other factors are considered."

RESPONSE

The study finds the two paragraphs of comment above conflicting in some respects. EPA states that its major reservation with respect to WASH-1400 is that it implies, by presenting curves that compare nuclear and nonnuclear accident risks, that nuclear reactor accident risks are acceptable. Although EPA recognizes that WASH-1400 has made no judgment on risk acceptability, it also states that WASH-1400 cannot and should not address the matter of nuclear accident risk acceptability and suggests (1) that WASH-1400 not be subject to the interpretation that it presumes acceptability of nuclear accident risks; (2) that the presentations be modified to qualify the risk comparisions by placing more emphasis on the fact that they are only a first step toward the evaluation of risk acceptability and that other factors must be considered; and (3) that the comparative risk curves might be confusing to the average reader.

The reason for presenting comparative risk curves, as discussed in sections 1.10, 2.4, and 7.5 of the Main Report, is to provide readers with some perspective from which to view potential nuclear reactor accident risks. Because low-probability risks are not a part of common experience, most people do not consciously consider low-probability risks and their potential consequences. It was felt that the average reader would find it useful to have this type of perspective on low-probability/high-consequence risks in our society. No judgment on acceptability was made or implied by the authors of WASH-1400. This was stated in sections 1.10 and 7.5 of the Main Report; the applicable paragraph of section 7.5 reads as follows:

"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."

EPA goes on to state that it is not accurate to compare acute fatalities with latent deaths or to omit latent deaths from comparisons of fatalities. This is, in fact, a troublesome matter that was considered with some care by the study. The study agrees with EPA that it is not accurate to compare acute fatalities with latent ones, as some have done. As indicated in section 2.4 of the Main Report, since there are also serious questions about the validity and wisdom of such comparisons, the study made no such comparisons.

The problem of placing radiation-induced latent cancer fatalities in perspective is especially difficult since it is well known that there are latent cancer fatalities attributable to many causes (air pollution, chemical agents, etc.) in our society. Although there are sufficient data available to create models that can predict, albeit with some uncertainty, latent effects due to irradiation, there is not sufficient information to do so for other carcinogenic agents. Thus the study chose, as indicated in section 5.5.4 of the Main Report, to compare the various radiation-induced latent effects with the normal incidence of similar effects. For instance, in connection with latent cancer fatalities, it is shown that the numbers predicted due to potential nuclear reactor accident represent a small fraction of the normal incidence of cancers due to other causes. While in this type of comparison potential latent effects from nuclear accidents are contrasted with those occurring principally from nonnuclear, environmental causes, the comparison provides some degree of perspective and is considered fair because some epidemiologists have estimated that the majority of normally occurring cancer fatalities are due to environmental causes.

The EPA suggestion that a better appreciation of the risk estimates could be gained if their uncertainties were added to the probability vs. consequence curves is correct. These uncertainties were shown on the curves for all the principal accident effects presented in chapter 5 of the Main Report. The uncertainties were not shown on the comparison curves in the draft report because they had been shown earlier in chapter 5. However, the comparison curves in the final report have been modified in this regard.

The study agrees with EPA that the risks from nuclear power involve not only those from potential reactor accidents

but also those due to normal reactor operation as well as considerations pertinent to the rest of the fuel cycle. These other matters are outside the scope of this study, as indicated in section 18 of this appendix; however, the published literature contains a significant body of analysis of many of those areas.

COMMENT 5

The area of human reliability appears to be improperly or incompletely considered.

RESPONSE

The EPA reference apparently results from a number of specific comments in the Intermountain Technologies, Inc., report. Section 14 of this appendix discusses the general approach used in the handling of human errors in the study, and section 5 dicusses some specific comments in this area. The study's position can be summarized as follows: the assignment of probabilities to human errors generally involves more subjective judgment than is used in other probability assignments; however, there is sufficient generalized information on human behavior to permit a valid quantification of human-error probabilities for use within the accuracies needed for risk assessment.

COMMENT 6

"The area of common mode failure, in particular, needs further elaboration, especially because the concept employed in the Reactor Safety Study seems to be broader and inclusive of a greater variety of failures than the usual interpretation of the term. The assertion that common mode failures do not contribute much to the overall risk needs extensive and substantial additional support in the form of comprehensive, logical, and well-connected coverage of the subject. The recent fire at the Browns Ferry plant, an example of a common mode failure which disabled a number of systems of two power reactors simultaneously, emphasizes the need for thorough examination of common mode failure."

RESPONSE

The study agrees with EPA that the matter of common mode failures needed further elaboration over the discussions provided in draft WASH-1400. These discussions were widely scattered through the various portions of the report and somewhat difficult to follow. Section 3 of this appendix has been provided in response to the many comments received in this regard. The discussion in section 3 provides an overview of the methodology used in the study and the ways in which common mode failures were handled. It has also been included as Addendum I to the final Main Report.

The recent fire at the Browns Ferry plant is indeed an example of a common mode equipment failure and has been analyzed in section 3.2 of this appendix and in section 5.3.4.4 of the Main Report. This analysis estimates that the probability of a potential core melt accident due to that fire was approximately 20% of that due to the other causes identified in the study. At that probability, the occurrence of the fire does not impact significantly on the validity of the study's results.

COMMENT 7

"The discussion of design adequacy needs to be expanded to include explicit description of the manner in which possible design inadequacies in components, structures, and systems are accounted for in the study methodology."

RESPONSE

As indicated in section 3.1.5 of this appendix and in Appendix III, the general as well as the nuclear failure data that were examined contained failures experienced in actual operation. Many system reliability predictions performed by others, where insufficient data were available from operating experience, used only partially applicable data obtained from bench or laboratory tests. Such data generally have inadequate content with respect to many characteristics of production line equipment used in field applications. The data obtained from field sources incorporate many causally related failures, such as those due to manufacturing and construction defects, design errors, quality control inefficiencies, environmental conditions, and human causes as well as a wide variety of other causes. Thus the failure rates used in the study were essentially total failure rates, and not simply "random" failure rates. Special common mode studies were thus not needed to identify failure causes that were already included in the data.

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.[1]

Certain nuclear components are required to remain operational under these conditions and are therefore designed to accommodate stresses of this type. Since neither nuclear or nonnuclear components generally experience these stresses, their effects are not included in the data sources used to derive failure rates for 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, there is no experience data 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 made. The results of this examination indicated some deficiencies (about 10%) 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 failure probability for safety systems under seismic loads, as indicated in section 5.4.1 of the Main Report.

COMMENT 8

The techniques for calculating the results of small pipe breaks in PWRs appear to be incompletely considered. The detailed basis for this comment is presented in the Intermountain Technologies, Inc., report which indicated that there may be inadequacies in the PWR vendor modeling of predicted peak clad temperatures.

RESPONSE

It appears, as indicated in the ITI report, that the concern in this area stems primarily from the following: the peak temperatures predicted by different PWR reactor manufacturers vary between 1100 and 1400 F, and it was difficult for ITI to establish the reasons for these differences because the details of the analytical techniques used are proprietary. However, the principal factor to consider in terms of the impact of these calculations on the results of the WASH-1400 risk assessment is that the temperature range cited is well below the NRC peak clad temperature limit of 2200 F. Thus, from the viewpoint of reactor accident risk assessment, the study believes that the expressed concern in this area is not germane.

COMMENT 9

"The core meltdown and containment response analyses in the draft WASH-1400 were found to contain many oversimplifying assumptions.... It appears that there are especially large uncertainties in knowledge of the behavior of the core and its surroundings once the core melting begins. The significance of the oversimplifying assumptions appears to be due to their influence on the probable sequence of events, i.e., whether the heating of the core is so rapid that it melts before effective cooling is restored, and, if effective cooling is not restored, whether the containment fails by excessive internal pressure or by some other mode. For example, in part of the containment failure analysis in draft WASH-1400, it is assumed that a molten core will generate considerable carbon dioxide gas by decomposition of foundation concrete containing limestone aggregate. The analysis of some possible accident sequences shows this gas providing sufficient additional internal pressure to fail the containment before the pressure is relieved into the ground by the molten core penetrating the foundation. The assumption that all foundations contain gas-generating aggregate appears to lead unrealistically to higher risk estimates."

RESPONSE

EPA is correct in saying that simplifying assumptions were made in the core heatup, core meltdown, and containment response analyses described in Appendix VIII. In a number of instances more sophisticated treatments could have been utilized, but they were not considered

---

[1]Tornado loadings did not play a large part in the analysis and are not discussed any further here. The details of the tornado design adequacy investigation are covered in Appendix X.

necessary. For example, in the calculation of surface heat transfer coefficients for the fuel pins during a LOCA, simplified treatments were found to be adequate because of (1) the essentially adiabatic nature of the heatup for rods that are not covered with water and (2) the close coupling of the fuel cladding temperatures to the water temperature in areas where the rods are water-covered. A detailed treatment taking into account time-dependent changes in physical properties and heat transfer coefficients would have had some effect on the time of core melting but little effect on the results of the analyses. For example, analyses performed by ITI indicate that the inception of core melting might have been calculated to start about 10 minutes earlier if more detailed calculations had been made. Such changes in timing could potentially affect the amount of radioactive decay prior to release or the time available for evacuation after a warning is given. However, considering that the isotopes that are large contributors to the predicted consequences have half-lives longer than 1 day, changes in timing of 10 minutes would not significantly affect the amount of radioactivity released. Similarly, the evacuation model used in assessing consequences (described in Appendix VI) is insensitive to small variations in timing. Thus, use of more sophisticated calculational techniques was not warranted.

With regard to the comment on restoration of cooling, it should be noted that the study assumed that if the emergency cooling injection system failed after a LOCA, restoration of core cooling would not prevent core melting. Because the fuel cladding reacts exothermically with steam as high fuel cladding temperatures are reached, the time interval available for remedial action is so small that credit cannot be given for remedial operator action.

As noted in the comment, the containment response analysis assumed the presence of a limestone concrete similar to that used at some plants, although it is not necessarily typical of the concrete used in all plants. Because of the high carbonate content of the concrete assumed, the calculations performed in Appendix VIII should provide an upper bound on the quantity of carbon dioxide and water generated by concrete decomposition during meltthrough. The study recognizes that certain plants use basaltic concretes that would not generate gases in the quantities calculated. Extrapolation of the study's results to such plants is therefore somewhat conservative. It should be noted, however, that the incremental gas contribution from concrete decomposition is relatively small for PWR analyses and the use of basaltic concrete would not significantly change the probabilities of overpressure failure or the timing associated with the various PWR sequences.

The role of noncondensable gases is more significant in the BWR LOCA sequences. In the analyses presented in Appendix VIII, carbon dioxide evolved on the decomposition of limestone concrete was found to be one of the principal contributors to containment overpressurization. If a basaltic concrete were to be used, no carbon dioxide would be generated. These analyses, however, considered only the hydrogen produced during the initial core melting (i.e., by the 50% reaction of zirconium with water).

Hydrogen would also be generated from reaction of the bulk of the remaining zirconium with water and the reaction of molten structural material with water after reactor vessel meltthrough.

The additional hydrogen would be sufficient to cause containment overpressure failure, even in the absence of carbon dioxide. Since the hydrogen generation rate is somewhat uncertain because it depends on the availability of water to the melt as well as the available surface area of the reactive materials in the melt, the time of containment failure may vary somewhat from that calculated when considering limestone concrete. It is clear, however, that overpressure failure would occur prior to containment meltthrough even under somewhat optimistic assumptions regarding the rate of hydrogen generation from the molten material. Thus, the containment failure modes for the various sequences would not change significantly if extrapolated to a BWR plant constructed of basaltic concrete.

COMMENT 10

"It would seem reasonable from the explanation in draft WASH-1400 of the

basis for selection of the pressure at which the containment of the example pressurized water reactor is assumed to fail under accident-created conditions to have selected a lower pressure. This explanation should be expanded to provide more justification for the high pressure selected, because in a number of possible accident sequences the failure pressure appears to be a determining factor relative to release of radioactivity to the atmosphere through the failed containment wall or release into the ground by the core melting through the foundation."

RESPONSE

The containment failure pressure of 100 psia determined by the study represents a nominal failure pressure for the containment. A containment failure probability of 0.5 was assigned for the calculated pressure of 100 psia. The containment failure probability was represented as a continuous variable with a normal distribution about this value.

It should be added here that the ITI report recommended a value of 67.5 psia for the minimum failure pressure. This is roughly equivalent to the 2σ lower bound of 70 psia used in the study. Appendix E to Appendix VIII has been rewritten to better clarify the approach taken and the rationale behind the nominal failure pressure selected.

COMMENT 11

"The draft WASH-1400 has also served to call attention to problems associated with the response to an accident to mitigate the consequences to the public. In dealing with an accidental release, the evacuation model of draft WASH-1400 includes a warning time for evacuation which apparently begins at the time of awareness of impending core melt. In order to show that the warning time for evacuation is determined on a practical basis, the final report should give examples of the limiting conditions in the plant which are postulated as bases for the decision to warn the neighboring population to evacuate, and the plant instrumentation indications that will tell the operator that the limiting conditions have been reached."

RESPONSE

The warning time for evacuation is defined as the interval from the time of awareness of impending core melt to the time of radioactive release to the atmosphere. It should be noted that the warning times would be only slightly longer than the interval between the inception of core melting and the time of containment failure. The operator can determine if the engineered safety systems are operating properly from the temperature and pressure drop information displayed in the control room. Furthermore, containment pressure is also monitored. Inception of core melting would be accompanied by an increase in the quantities of radioactivity released to the containment in certain accident sequences. This would be detectable from outside containment by means of appropriate portable monitors or by sampling the containment atmosphere.

It should be noted that section 7.4.2 of the Main Report suggests that steps be taken to ensure that existing evacuation plans at nuclear power plants include requirements for instrumentation and monitoring pertinent to evacuation warnings.

COMMENT 12

"...The consequence modeling assumptions appear to underestimate the health effects resulting from the accident sequences associated with the larger releases of radioactivity."

RESPONSE

The Reactor Safety Study's reevaluation of draft WASH-1400 and the comments received indicated that the draft consequence model had some deficiencies and some errors. Therefore, an improved consequence model was developed as a part of the final report. This model is described briefly in section 4 of this appendix and in great detail in Appendix VI. The results of calculations of the effects of potential nuclear reactor accidents are presented in chapters 5 and 7 of the Main Report. Section 4 of this appendix includes a comparison of the values computed in the draft and final reports.

2.2 AMERICAN PHYSICAL SOCIETY STUDY GROUP ON REACTOR SAFETY

A special American Physical Society Study Group on Reactor Safety published certain principal observations concerning draft WASH-1400 in the Reviews of Modern Physics, volume 47, Supplement No. 1 (summer 1975). These observations are presented in this section together with the study's responses.

COMMENT 1

"We did not have the resources to carry out an independent evaluation of this aspect of the recent AEC Reactor Safety Study (Draft WASH-1400), but we recognize that the event-tree and fault-tree approach can have merit in highlighting relative strengths and weaknesses of reactor systems, particularly through comparison of different sequences of reactor behavior. However, based on our experience with problems of this nature involving very low probabilities, we do not now have confidence in the presently calculated absolute values of the probabilities of the various branches."

RESPONSE

The American Physical Society Study Group on Reactor Safety (APSSG) statement that it lacks confidence in the ability to properly calculate the absolute values of events having low probabilities is somewhat understandable. As indicated in section 1.2 of the Main Report, "at the start of the Reactor Safety Study... 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 up to that time 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."

However, it is important to understand the insights gained from the overall accident sequences developed in WASH-1400. As discussed in section 3.1.2.3 of this appendix, most of the accident sequences that contributed to the overall risk of reactor accidents are of the form $P_{IE} \times P_{SF} \times P_{CFM} \times P_{WC} \times P_{PD}$.[1] It is noted that this formulation was carefully examined for potential dependencies between the various failure modes and indicates how they were handled. It is also noted that the values for P_{IE}, P_{WC}, and P_{PD} were established on the basis of experience and measured data. The fault tree methodology is applicable only to one element, P_{SF}, whose contribution to the overall accident sequence probability is, in general, only about 10^{-2}. P_{CFM} clearly represents the dependent failure of containment due to core melt resulting from the combination of $P_{IE} \times P_{SF}$ and can generally be thought of as having a value of 10^{-1}. Thus the entire engineering contribution to accident sequence probabilities of 10^{-9} that have large consequences is only about 10^{-3}.

This relatively small contribution of safety systems and containment to the overall probability of large consequence accidents is an extremely important new perspective, derived principally from the event tree methodology described in section 3.1.2.1 of this appendix.[2] The five-factor formulation indicates that no single factor in an accident sequence dominates the determination of risk and that the engineering factors analyzed by fault tree methodology represent only one of the five factors. Thus, the use of fault tree methodology, per se, does not play a dominant role in the overall quantification of risk.

Nevertheless, every effort was made in WASH-1400 to complete an adequate quantification of the prediction of system failure probabilities by fault trees, as described in section 3.1.2.2 of this appendix. Previous work by others in predicting the unavailability of engineered systems often yielded values of 10^{-9} to 10^{-8} or less. These unrealistically low values have led some people to hold the view that the prediction of excessively small failure probabilities is an inherent characteristic of fault

---

[1] P_{IE} = probability of an initiating event; P_{SF} = probability of failure of a safety system such that when combined with P_{IE}, produces core melt; P_{CFM} = probability of containment failure in one of a number of risks, given core melt; P_{WC} = probability distribution of weather conditions; P_{PD} = probability distribution of people exposed to radioactivity.

[2] There is no intention here of denigrating the importance of having highly reliable safety systems for use in nuclear power plants.

tree methodology. Section 3.1.1 of this appendix presents the views and experience of the National Aeronautics and Space Administration, the U.S. Environmental Protection Agency, the Systems Reliability Service of the United Kingdom Atomic Energy Authority, and the Reactor Safety Study--views indicating that the methodology can and has produced credible estimates of system failure probability. Section 3.1.2.2 (para. 3) also indicates that the values obtained for fault tree predictions in WASH-1400 generally fell in the 10^{-4} to 10^{-2} range. These values are significantly higher than those early results of others mentioned above and are in agreement with those that were obtainable from experience.

COMMENT 2

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

RESPONSE

An improved consequence model has been developed as a part of the final WASH-1400 report (see response to comment 12 in section 2.1 of this appendix).

COMMENT 3

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

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

RESPONSE

As pointed out in section 1 of Appendix II, in the draft report and section 3.1.1 of this appendix, the results of the study's fault tree predictions of system and subsystem failures were checked against failure data derived from experience with operating reactors. In those cases where data were available, the predictions matched the data within about a factor of 2, which is within the confidence bounds associated with these values.

The study concurs with the suggestion that future effort by the U.S. NRC be devoted to further parametric studies and refinements of the WASH-1400 work.

2.3 U.S. ATOMIC ENERGY COMMISSION REGULATORY STAFF

The AEC Regulatory Staffs' review of draft WASH-1400 was received on December 2, 1974. This review was performed by a Regulatory Staff task force, which was augmented with outside consultants. The detailed review by the Regulatory Staff and their comments were a significant aid in preparing the final report. The Regulatory Staff's principal comments are presented below together with the Study's responses where appropriate.

COMMENT 1

"We believe that the Study represents a significant breakthrough in the quantitative evaluation of the risk to the public from nuclear power plants. This work is by far the most comprehensive, systematic, quantitative effort yet conducted in this field. It provides information of a new dimension to assist in making informed decisions when the risk is a significant consideration. It is therefore an important step in the evolution of safety technology."

COMMENT 2

"The comparison of nuclear and non-nuclear risks is a useful yardstick to calibrate the reader's understanding of the probability results, but the treatment of risks should be more consistent regarding onsite effects.... The Study results in the area of individual risks would be more precise if they included as a refinement the large variability of such risks to the individual arising from, for example, differences in proximity to nuclear plants or differences in proximity to dams...."

RESPONSE

Since the principal objective of the Reactor Safety Study was to perform a quantitative assessment of the risk to the public from reactor accidents,

onsite effects, such as property damage to the plant itself, were not included in the calculations. However, even if they had been included, the overall results of the study would not have been affected significantly.

In regard to variability in individual risk as a function of distance from the plant, Appendix VI, section 13 has been modified to include such considerations.

COMMENT 3

"...Some quite conservative (overly pessimistic) assumptions were made... regarding the frequency of several initiating events and the criteria for the successful operation of several engineering safety features. Other assumptions, whose realism is difficult to evaluate, were necessarily made in core meltdown and containment failure [sequences], where the available technology base is not as firm as in other parts of the calculations. Specifically, we believe that the frequency of core meltdown given in the study is substantially higher than reality, as are the frequencies given for many of the initiating events and the probabilities given from some of the system failures."

RESPONSE

Where information was available, the study attempted to treat physical phenomena in a realistic manner. In some areas, such as the phenomena associated with core meltdown and containment failure modes, where data are sparse, the study attempted to ensure that its calculations were not unconservative. Furthermore, it is believed that the rather large error spreads resulting from the analysis would cover more realistic values. As additional data become available, future studies may well be able to perform more realistic analyses, if they are deemed necessary.

COMMENT 4

"The explicit inclusion of human error in the fault trees is an important improvement over previous evaluations, as is the comprehensive and detailed consideration given to common mode failures in all phases of the calculations. The latter would be improved, however, by explicit inclusion of related failures attributable to design and manufacturing errors, over and above the "failure-rate coupling"...now included."

RESPONSE

See section 3.1.4 of this appendix for a full discussion of the handling of common mode failures in the fault trees used in this study and the response to comment 7 in section 2.1 of this appendix for a discussion of the incorporation of failures attributable to design and manufacturing errors.

COMMENT 5

It was indicated that two events had been identified that could potentially affect the results of the Reactor Safety Study: a control rod ejection accident in the BWR and a seismic event more severe than the safe shutdown earthquake (SSE).

RESPONSE

Draft WASH-1400 addressed potential rod ejection accidents in BWRs and indicated that their contribution to overall accident risks would be essentially negligible because of their low probability of occurrence compared to potential accidents that have similar consequences. Because of the interest in this matter by the Regulatory Staff and others, an expanded analysis of a potential rod ejection accident is presented in section 9 of this appendix.

The discussion of severe seismic events in section 5.4.1 of the draft Main Report did not include a complete analysis of the potential effects on potential accident risks of earthquakes larger than the safe shutdown earthquake. This section has been rewritten in the final report to include these considerations in the analysis. However, the conclusion that earthquakes are not expected to contribute significantly to reactor accident risks remains unchanged.

COMMENT 6

"The probability and consequences of the release of significant amounts of nonvolatile material to the environment during postulated disruptive events have not been adequately addressed. The results of alternative health effects assumptions and the effect on the results of inclusion of the cost of illnesses should be more thoroughly presented."

RESPONSE

An improved consequence model was developed as a part of the final report

(see response to comment 12 in section 2.1 of this appendix).

COMMENT 7

"...More information on determining the degree of sensitivity of the [consequence model] results to [potential variations in] the various factors would be valuable... A systematic discussion of which quantities are important and which, if altered, would change the results, would be helpful."

RESPONSE

Sensitivity studies that are broader in scope than those performed in draft WASH-1400 would indeed be useful. Studies of this type require an extensive and careful effort to ensure that the variations in consequences that are produced are associated with correctly stated variations in probability. Studies involving simultaneous variations in multiple parameters are even more difficult.

The sensitivity studies reported in Appendix VI are of a more limited nature. They involve the variations in single parameters that the study considers useful in lending additional qualitative perspective to the results of the overall consequence calculations. This is true even though in some cases variations in probabilities associated with these potential changes in consequences could not be determined.

More precise and broader sensitivity studies should be performed in future work of this type.

2.4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

The ACRS review of draft WASH-1400 was received on April 8, 1975. The ACRS summary and the study's response are presented below.

"The ACRS believes that the RSS represents a valuable contribution to the understanding of light water reactor safety in its categorization of hypothetical accidents, identification of potential weak links for the two reactors studied, and its efforts to develop comparative and quantitative risk assessments for accident sequences examined. The Committee believes that a continuing effort and better data will be required to evaluate the validity of the quantitative results in absolute terms. Special emphasis should be given to quantification of the initiators, probabilities, and consequences of core melting.

"The Committee believes that the methodology of the RSS should be applied to other types and designs of reactors, other site conditions and other accident initiators and sequences, and that the current efforts to compile, categorize, and evaluate nuclear experience should be extended in breadth and depth to improve the data base for future studies of this type.

"The Committee believes, further, that the RSS can serve as a model for similar studies of the failure probabilities, consequences, and resulting risks of other hazards (both nuclear and nonnuclear) to the health and safety of the public.

"The Committee believes that many of the techniques used in the RSS can and should be used by reactor designers to improve safety and by the NRC Staff as a supplement to safety assessment.

"The Committee's review of the RSS has not caused the Committee to alter its judgment that reactors now under construction or in operation do not represent undue risks to the health and safety of the public."

RESPONSE

The study agrees with the ACRS that efforts of the type reported in WASH-1400 should be continued in the future and that risk assessments of the same type should be performed in connection with advanced reactor designs such as the liquid metal fast breeder reactor and the high temperature gas reactor at an appropriate time.[1] While the study believes that the extrapolation of the results of the analysis of two reactors to the first 100 large light-water-cooled plants is generally valid and that the data base used in WASH-1400 for estimating accident sequence probabilities is adequate for the purpose

[1] A full-scale risk assessment effort as detailed as that performed in WASH-1400 probably could not be undertaken now because of the lack of sufficiently detailed information. However, some work in the construction of event trees, and possibly some fault trees would probably be useful.

intended, draft WASH-1400 made the following suggestions, as indicated in section 7.4.2 of the Main Report:

1. It would be useful in the future to pursue the variations in design from plant to plant and from site to site that could potentially affect the applicability of the WASH-1400 results to 100 reactors.

2. It would be useful to collect more data on nuclear plant operating experience for use in future reliability and risk assessments.

The study further believes that a WASH-1400 type assessment of water reactors should be repeated in approximately 5 years. The intervening period should permit the collection of additional nuclear power plant failure rate data and the further development of the methodology to permit more precise assessments to be performed. It is important that the collection of data and the development of methodology be pursued vigorously if these goals are to be achieved.

Although the ACRS suggests that many of the techniques used in WASH-1400 can be used to improve reactor safety, WASH-1400 does not address the need for improvement or relaxation in reactor safety requirements. This type of decision should be made in another forum, as already stated in section 7.5 of the Main Report.

2.5 UNION OF CONCERNED SCIENTISTS (UCS)

The Union of Concerned Scientists' comments on draft WASH-1400 were received on November 22, 1974. The UCS review was made in conjunction with the Sierra Club, and the review team consisted of a task force of 10 scientists and engineers from these organizations. It was pointed out that, due to the inadequate time provided for review, the comments were preliminary and the conclusions somewhat tentative. No final comments had been received as of October 15, 1975.

The six conclusions made in the UCS/Sierra Club review and a discussion of these conclusions are presented below. All elements of the UCS/Sierra Club review were carefully considered in the preparation of the final report. Specific UCS comments of a more limited nature are discussed later in this appendix.

CONCLUSION 1

"We have concluded that the event tree/fault methodology if properly utilized can be very helpful in making comparisons between diverse system designs, assessing relative improvements from system component changes, or identifying design weak points. We do not believe, however, that the methods can be employed as RSS has done to determine absolute probability values for accident probabilities and to use these predictions as proof of the safety of nuclear plants. The many and important residual uncertainties introduced by use of the methodology make this RSS application technically unsound and unjustified. Experience with manned and unmanned space mission applications of these methods fully supports our conclusions."

RESPONSE

The safety study staff believes that the methodology developed and utilized for WASH-1400 can and does provide meaningful results to aid in the evaluation of nuclear accident probabilities and associated consequences. This belief has been confirmed by others, as indicated in section 3.1.1 of this appendix. Section 3 of this appendix provides an overview of the WASH-1400 methodology that readers will find helpful in determining the validity of the methodology and its application.

CONCLUSION 2

"We have concluded that the aggregate consequences to human health of major accidents evaluated by RSS are seriously under-stated. We can conservatively account for a factor of 16 in regard to fatalities and acute illness. The value may well be higher. Reevaluation of RSS results, correcting only for this error, using RSS methods, establishes that the probability of killing 2300 persons and injuring 5600 more in an accident is increased over the RSS value by a factor of 400. The accident probability assigned by RSS to an accident of that size is, on reevaluation of the consequences, found to be the probability of an accident in which 37,000 people are killed and 90,000 made acutely ill. Similar results occur for cancers, genetic damage, thyroid illnesses, and property damage."

RESPONSE

An improved consequence model has been developed as a part of the final report

(see response to comment 12 in section 2.1 of this appendix).

CONCLUSION 3

"There are serious implications of RSS results for the country's nuclear program that are either ignored or incorrectly stated in the RSS report.

"1. The concept of floating, or offshore, nuclear power plants is seriously damaged, based on the RSS probability of reactor core melting of 1 in 17,000 reactor years. This concept is presently being implemented and a number of plants have been ordered. No protective features are available for floating nuclear plants to prevent immense and persistent damage to the oceans in the event of a meltdown accident. The RSS probability is unacceptably large. No mention of floating plants is made in RSS.

"2. The consequences and the risk from sabotage are seriously understated. RSS does not address the problem of determining the probability of sabotage or of means of preventing or mitigating it, an important omission. RSS does, however, state that the consequences will be no worse than those accidents they studied. We conclude this to be incorrect owing to our conclusion that an act of intentional and malevolent ill will can frustrate a great many of the normal factors which can act to ameliorate the size and consequences of a radioactive release. Accordingly, sabotage is felt by us to be able to induce immense damage and is an issue of great importance.

"We conclude that there are serious implications concerning the nuclear program to be drawn from RSS results that the report fails to acknowledge."

RESPONSE

Apparently the UCS overlooked section 1.9 of the Main Report of draft WASH-1400, which pointed out that the scope of the study included "only light water cooled nuclear power plants of the type now coming into operation." The study's results have been extrapolated to cover only the first 100 large nuclear power plants, which do not include offshore plants. This matter is discussed in greater detail in section 18 of this appendix.

The draft report was somewhat unclear in its statements about the coverage that had been given to the matter of potential sabotage. Further information that has become available has also been added to the report. Sections 1.9(3), 5.4.6, and 7.4.2 of the Main Report have been clarified in this regard. These discussions are summarized in section 16 of this appendix.

CONCLUSION 4

"We have concluded that the new RSS conclusions, even though based in part on weak or inadequately documented evidence, call into most serious question the competence of the AEC in its conduct of safety analyses on which for a decade or more the major safety assurances of the nuclear program have been based. The RSS, both explicitly and implicitly, admits the existence of significant defects in these analyses."

RESPONSE

Contrary to the above view, the study group believes that WASH-1400 provides confirmation of the care and thoroughness exercised by large numbers of dedicated personnel in industry and government in having achieved the relatively low levels of potential risks in commercial nuclear power plants that the study calculated. This belief was stated in slightly different words in section 7.1 of the draft Main Report as follows:

"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 is engaged. Although the study has developed some insights that contribute to a better understanding of reactor safety, the existing relatively low level of risk has been achieved principally by the effort of industrial design, construction and operation and by the efforts of the AEC's regulatory process."

CONCLUSION 5

"We conclude that RSS did not take advantage of opportunities to verify the capacity of a newly applied and controversial methodology to contribute to risk assessment. This is an important defect. We further conclude that as a consequence the public is now asked, again, to believe in unverified and inadequately-supported computer-supported predictions."

RESPONSE

As discussed in section 1 of Appendix II, volume 1, of the draft report, the study obtained data from field experience on two systems that were similar to corresponding systems being evaluated. The predicted probabilities of failures for these systems were in good agreement with the actual values. Other organizations, such as the Systems Reliability Service in the United Kingdom, have had experience in quantitative reliability prediction techniques and have found the results of these prediction techniques to be in good agreement with experience. See section 3.1.1 of this appendix for a more complete discussion of this matter.

CONCLUSION 6

"We have concluded that the AEC's use of this report is improper and wrong, and that the report, because of its limitations and defects cannot be used to sweep away the doubts about reactor safety. We have finally concluded that the nuclear program is in great need of a substantial, highly competent, and disinterested review of all aspects of the program's potential impact on public safety. The USAEC's inhouse Reactor Safety Study will not serve. It was not disinterested, and it is technically flawed, and its results are being misused."

RESPONSE

WASH-1400 is a technical report prepared by persons recognized to be competent in their fields, and the study believes it is inappropriate for it to enter into consideration of motivations. The safety record of nuclear reactors has so far been excellent, and the projected potential risks are predicted to be comparatively small. The report has in essence been reviewed as suggested by UCS. A broad spectrum of our society, representing many diverse veiwpoints and fields of expertise, has been asked to comment on draft WASH-1400, and comments were received from additional sources as well. Especially thorough reviews appear to have been conducted of the consequence area by such organizations such as the U.S. Environmental Protection Agency, the U.S. Atomic Energy Commission Regulatory Staff, the American Physical Society Study Group on Reactor Safety, and Resources for the Future, Inc. Deficiencies and errors in the consequence model have been corrected. The results of calculations obtained with the revised consequence model are compared with earlier results in section 3 of this appendix.

2.6 RESOURCES FOR THE FUTURE, INC.

The Resources for the Future, Inc., review was received on November 6, 1974. This review also incorporated a review of Appendix VI made by one of the staff members of the National Resources Defense Council, Inc. The detailed comments received concerning Appendix VI were a significant aid in updating the consequence model for use in the preparation of the final report.

The main points of the Resources for the Future, Inc., review are as follows:

SUMMARY 1

"Turning to the broader questions raised by our reading of the report, two strike us as of special importance. The first is the exclusion of the deliberate acts of operating personnel from the scope of the study. While there are obvious analytical reasons for distinguishing technological risks associated with system failures from risks associated with system failures initiated or compounded by deliberate operator actions, the latter are very possibly more important than the former. Their explicit inclusion in any overall risk assessment of this light water reactor is essential."

RESPONSE

The draft report was somewhat unclear in its statements about the coverage that had been given to the matter of potential sabotage. Further information that has become available has also been added to the report. Sections 1.9(3), 5.4.6, and 7.4.2 of the Main Report have been clarified in this regard. These discussions are summarized in section 16 of this appendix.

SUMMARY 2

"The second broad question raised by our reading of the report and by the interpretations of the report given the broadest currency concerns the emphasis thereby given to what is only a part of the uranium fuel cycle. The risks relevant to overall technological risk assessment are of course the risks associated with the entire cycle. In what appears to be a disproportionate allocation of risk assessment effort to what may be a relatively low risk part of the cycle, other risks -- notably those associated with the transport of hazardous materials and the diversion of hazardous materials -- may be left unestimated, and therefore be underemphasized and underestimated."

RESPONSE

Section 1.9 of the Main Report of draft WASH-1400 pointed out that the scope of the study included "only light water cooled nuclear power plants of the type now coming into operation." Its results have been extrapolated to cover only the first 100 large nuclear power plants and do not include those risks associated with the transportation of hazardous materials and the diversion of hazardous materials. This matter is discussed in greater detail in section 17 of this appendix.

SUMMARY 3

"Among the narrower and more technical questions raised in our reading of the report we can perhaps point to Appendix VI, "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," as one source of our concern that the technical apparatus of the report -- the data base assembled and the models employed -- be subject to a thorough review. We have appended to this letter a list of what we believe are questionable assumptions and procedures employed in this Appendix. That list is intended to be suggestive rather than comprehensive, and is not to be taken as our final comment on either Appendix VI or the overall report."

RESPONSE

An improved consequence model has been developed as a part of the final report (see response to comment 12 in section 2.1 of this appendix).

Section 3

Reactor Safety Study Methodology

A large number of comments received from many sources concerned the methodology used in the study. These comments addressed both the general adequacy of the methodology as well as individual items of a more specific nature. The discussion that follows is divided into two parts: the first covers the adequacy of the overall methodology and the second covers the more specific points.

3.1 ADEQUACY OF THE OVERALL METHODOLOGY USED IN THE REACTOR SAFETY STUDY

The principal comments received concerning the adequacy of WASH-1400 methodology pertain to:

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

d. whether adequate failure rate data was available to quantify fault trees

Comment 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 3.1.1 and 3.1.2.2 will discuss the adequacy of fault tree methodology.

Comments 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 sequences in these nuclear power plants. These include interrelationships among the functions to be performed, between the functions and 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 3.1.2 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 3.1.3 examines the way in which the study determined the accident sequences of significance. Section 3.1.4 describes the data base used in the quantification of the event trees and fault trees. Finally, section 3.1.5 presents some modeling considerations associated with event trees and fault trees.

3.1.1 ADEQUACY OF FAULT TREE METHODOLOGY

Many comments[3] were received that challenged the conceptual adequacy of fault tree methodology. The principal point of these comments was that fault tree analysis is incomplete and is unable to produce reliable quantitative predictions of system failure probability. It was 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 were:

---

[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.

[3] Holmes & Narver, Inc.; Iowa Student Public Interest Research Group; Union of Concerned Scientists; Department of Health, Education and Welfare; Pollution & Environmental Control Problems, Inc.; Resources for the Future, Inc.; Amory Lovins; William M. Bryan.

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 comments, it is instructive to review those viewpoints that support the adequacy of fault tree methodology before proceeding with the technical response to the principal comments.[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.[3,4] 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[5] 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 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."

. . . . .

---

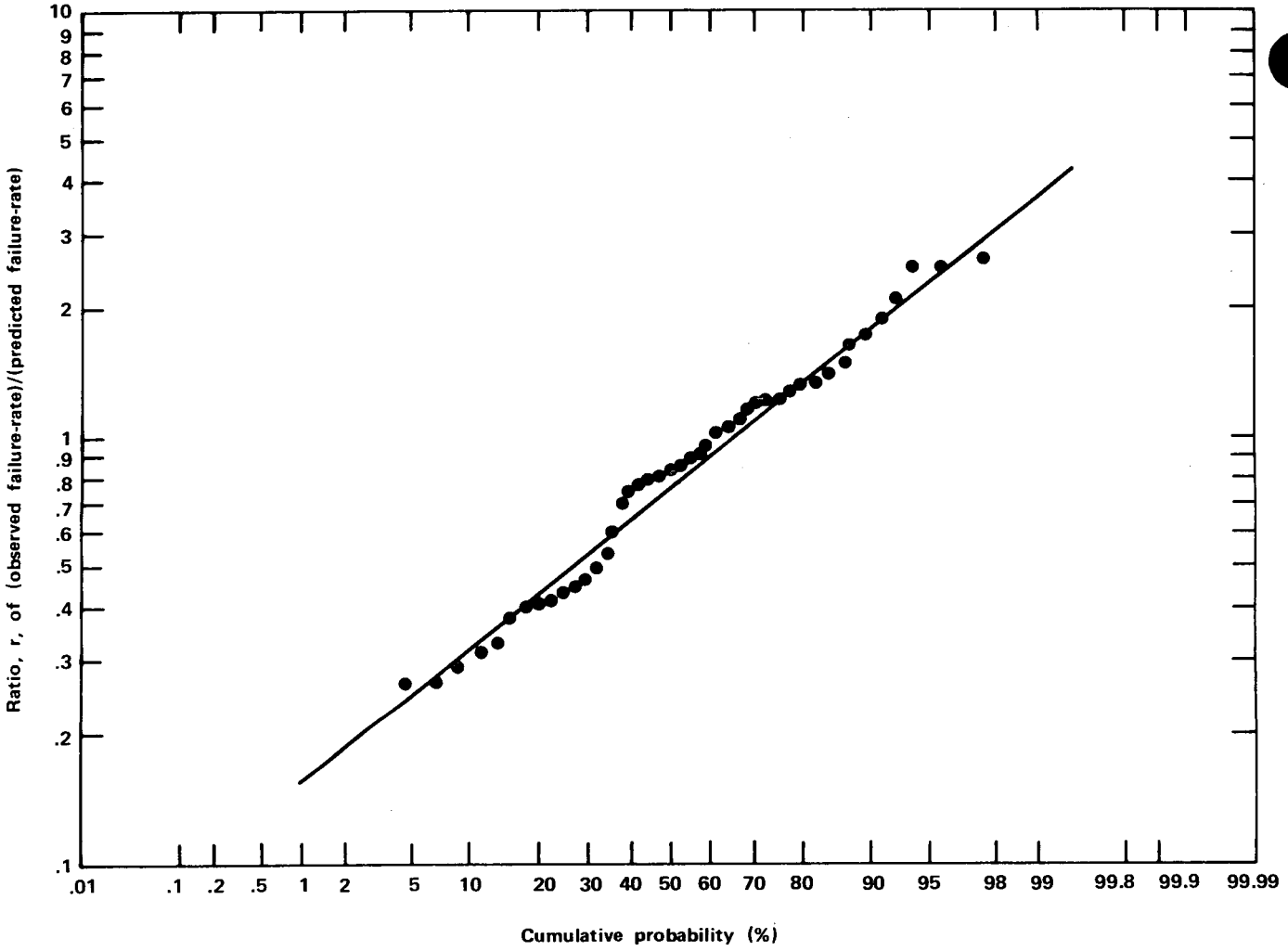
[1] The procedures used in the study to help ensure the completeness of fault trees and to achieve their reliable quantification are described in section 3.1.2.2.

[2] This letter is appended to this section as Attachment 1.

[3] A. E. Green and A. J. Bourne, Reliability Technology, Wiley-Interscience, London, 1972.

[4] Mr. Green's letter is appended to this section as Attachment 2.

[5] This letter also contained some specific criticisms of WASH-1400 that are addressed in section 2 of this appendix.



"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 contractors or laboratories to

[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 section as Attachment 3.

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 study believes this because 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.[2] 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 3.1.2.2.

The discussion that follows in the next several sections addresses in greater detail many of the more specific reservations that have been expressed about 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.

[2] It should be noted that, of those mentioned here, only the EPA (through a contractor, Intermountain Technologies, Inc.) performed some checking of the study's fault tree results.

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

James C. Fletcher
Administrator

Attachment 2

SYSTEMS RELIABILITY SERVICE
A service to industry operated by the United Kingdom Atomic Energy Authority.

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.

Our ref: SRS/POL/5/2
Your ref: AEG/27

Please reply to: Culcheth

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 Elettroteonico 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:

B-164105

> "* * * 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.

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

3.1.2 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.

3.1.2.1 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.

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

---

[1] Main Report, section 1.7 c.

[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.

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 XI 3-1 shows the possible choices of success or failure of each of the functions involved in potential LOCA accident sequences. Figure XI 3-2 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 would melt from the failure of reactor trip alone. Where 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.

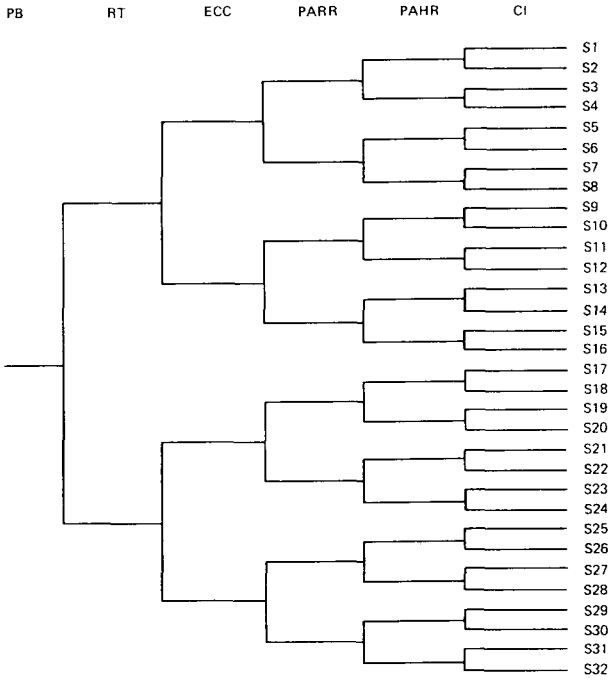


Fig. XI 3-1. Illustrative Event Tree for LOCA Functions

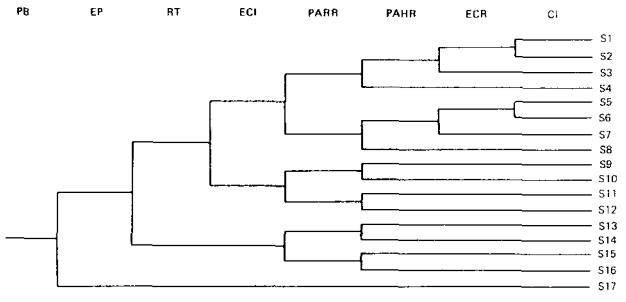


Fig. XI 3-2. Functional LOCA Event Tree Showing Effects of Interrelationships

---

[1] Figures I 2-1 and I 2-8 are reproduced here for the convenience of the reader as Figs. XI 3-1 and XI 3-2, 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.

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. XI 3-1 to that in Fig. XI 3-2 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. XI 3-1, 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 over 100,000 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.

Figure XI 3-3 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 probability discrimination technique has

---

[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] Figure XI 3-3 is 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 V 3-4 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 1×10^{-11} AF-α 1×10^{-10} ACD-α 5×10^{-11} AG-α 9×10^{-11}	AB-γ 1×10^{-10} AHF-γ 2×10^{-11} AB-δ 4×10^{-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} ADF-ε 2×10^{-10} AHF-ε 1×10^{-10}	AD-ε 2×10^{-6} AH-ε 1×10^{-6}	A-β 2×10^{-7}	A 1×10^{-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.

Fig. XI 3-3. Reproduction of Table V 3-4 of Appendix V

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).

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.[2] 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.[3] Potential common mode failures between systems and their components thus need be considered in only the remaining 27 sequences. Examination of Fig. XI 3-4 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.[4]

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 3.1.2.2, 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 Fig. XI 3-4, 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.

---

[1] See Fig. XI 3-4 which is Table 3-14 of Appendix V. The number of sequences (78) does not include sequences in which fuel melting does not occur.

[2] 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 3.1.2.3 of this appendix. 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.

[3] There are three single-event accident sequences in which system failures do not appear. These involve the check valve and reactor vessel rupture cases.

[4] The 27 sequences did not involve any combinations having more than two system failures per sequence.

TABLE V 3-14 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 $1x10^{-11}$ AF-α $1x10^{-10}$ ACD-α $5x10^{-11}$ AC-α $9x10^{-11}$	AB-γ $1x10^{-10}$ AB-δ $4x10^{-11}$ AHF-γ $2x10^{-11}$	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 $1x10^{-9}$ AHF-ε $1x10^{-10}$ ADF-ε $2x10^{-10}$	AD-ε $2x10^{-6}$ AH-ε $1x10^{-6}$	A-β $2x10^{-7}$	A $1x10^{-4}$
A Probabilities	$2x10^{-9}$	$1x10^{-8}$	$1x10^{-7}$	$1x10^{-8}$	$4x10^{-8}$	$3x10^{-7}$	$3x10^{-6}$	$1x10^{-5}$	$1x10^{-4}$
SMALL LOCA S_1	S_1B-α $3x10^{-11}$ S_1CD-α $7x10^{-11}$ S_1F-α $3x10^{-10}$ S_1G-α $3x10^{-10}$	S_1B-γ $4x10^{-10}$ S_1B-δ $1x10^{-10}$ S_1HF-γ $6x10^{-11}$	S_1D-α $3x10^{-8}$ S_1H-α $3x10^{-8}$ S_1F-δ $3x10^{-8}$ S_1G-δ $3x10^{-8}$	S_1CD-β $1x10^{-11}$	S_1H-β $5x10^{-9}$ S_1D-β $6x10^{-9}$	S_1DF-ε $3x10^{-10}$ S_1B-ε $2x10^{-9}$ S_1HF-ε $4x10^{-10}$	S_1D-ε $3x10^{-6}$ S_1H-ε $3x10^{-6}$	S_1-β $6x10^{-7}$	S_1 $3x10^{-4}$
S_1 Probabilities	$3x10^{-9}$	$2x10^{-8}$	$2x10^{-7}$	$3x10^{-8}$	$8x10^{-8}$	$6x10^{-7}$	$6x10^{-6}$	$3x10^{-5}$	$3x10^{-4}$
SMALL LOCA S_2	S_2B-α $1x10^{-10}$ S_2F-α $1x10^{-9}$ S_2CD-α $2x10^{-10}$ S_2G-α $9x10^{-10}$ S_2C-α $2x10^{-8}$	S_2B-γ $1x10^{-9}$ S_2HF-γ $2x10^{-10}$ S_2B-δ $4x10^{-10}$	S_2D-α $9x10^{-8}$ S_2H-α $6x10^{-8}$ S_2F-δ $1x10^{-7}$ S_2C-δ $2x10^{-6}$ S_2G-δ $9x10^{-8}$	S_2DG-β $1x10^{-12}$	S_2D-β $2x10^{-8}$ S_2H-β $1x10^{-8}$	S_2B-ε $8x10^{-9}$ S_2CD-ε $2x10^{-8}$ S_2HF-ε $1x10^{-9}$	S_2D-ε $9x10^{-6}$ S_2H-ε $6x10^{-6}$		
S_2 Probabilities	$1x10^{-7}$	$3x10^{-7}$	$3x10^{-6}$	$3x10^{-7}$	$3x10^{-7}$	$2x10^{-6}$	$2x10^{-5}$		
REACTOR VESSEL RUPTURE - R	RC-α $2x10^{-12}$	RC-γ $3x10^{-11}$ RF-δ $1x10^{-11}$ RC-δ $1x10^{-12}$	R-α $1x10^{-9}$				R-ε $1x10^{-7}$		
R Probabilities	$2x10^{-11}$	$1x10^{-10}$	$1x10^{-9}$	$2x10^{-10}$	$1x10^{-9}$	$1x10^{-8}$	$1x10^{-7}$		
INTERFACING SYSTEMS LOCA (CHECK VALVE) - V		V $4x10^{-6}$							
V Probabilities	$4x10^{-7}$	$4x10^{-6}$	$4x10^{-7}$	$4x10^{-8}$					
TRANSIENT EVENT - T	TMLB'-α $3x10^{-8}$	TMLB'-γ $7x10^{-7}$ TMLB'-δ $2x10^{-6}$	TML-α $6x10^{-8}$ TKQ-α $3x10^{-8}$ TKMQ-α $1x10^{-8}$		TML-β $3x10^{-10}$ TKQ-β $3x10^{-10}$	TMLB'-ε $6x10^{-7}$	TML-ε $6x10^{-6}$ TKQ-ε $3x10^{-6}$ TKMQ-ε $1x10^{-6}$		
T Probabilities	$3x10^{-7}$	$3x10^{-6}$	$4x10^{-7}$	$7x10^{-8}$	$2x10^{-7}$	$2x10^{-6}$	$1x10^{-5}$		
(Σ) SUMMATION OF ALL ACCIDENT SEQUENCES PER RELEASE CATEGORY									
MEDIAN (50% VALUE)	$9x10^{-7}$	$8x10^{-6}$	$4x10^{-6}$	$5x10^{-7}$	$7x10^{-7}$	$6x10^{-6}$	$4x10^{-5}$	$4x10^{-5}$	$4x10^{-4}$
LOWER BOUND (5% VALUE)	$9x10^{-8}$	$8x10^{-7}$	$6x10^{-7}$	$9x10^{-8}$	$2x10^{-7}$	$2x10^{-6}$	$1x10^{-5}$	$4x10^{-6}$	$4x10^{-5}$
UPPER BOUND (95% VALUE)	$9x10^{-6}$	$8x10^{-5}$	$4x10^{-5}$	$5x10^{-6}$	$4x10^{-6}$	$2x10^{-5}$	$2x10^{-4}$	$4x10^{-4}$	$4x10^{-3}$

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 (See Section 4.1).

Fig. XI 3-4. Reproduction of Table V 3-14 of Appendix V

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 Fig. XI 3-4), 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 XI 3-5 illustrates the net effect of the smoothing technique and shows that the probabilities of occurrence of several release categories were significantly increased.[1] It is interesting to note that, with the use of smoothing, the cumulative probabilities for all core melt release categories shown in Fig. XI 3-4 are principally determined by only six sequences.[2] 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 2 involve only one double system failure (ML).

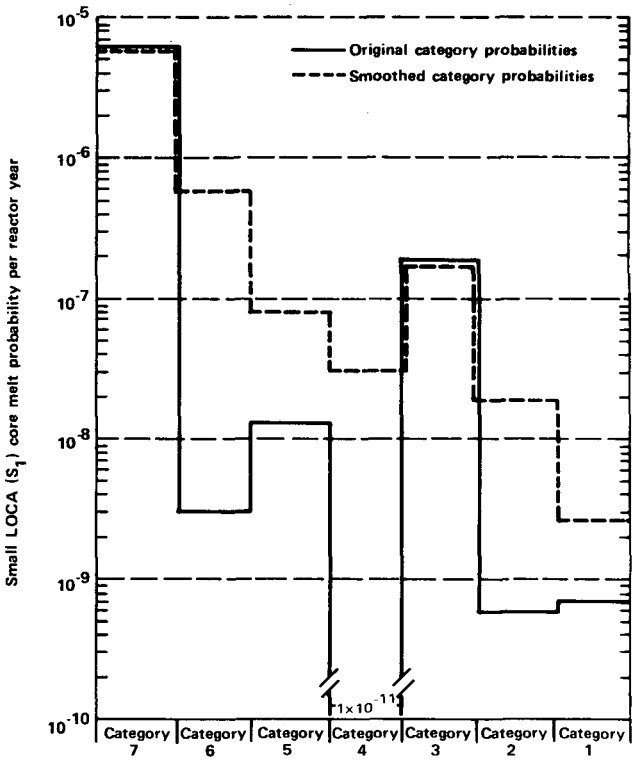


Fig. XI 3-5. Application of Probability Smoothing

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.[3] 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 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.

---

[1] This figure is the same as Fig. V 4-1 of Appendix V.

[2] S_2D_ε, S_2H_ε, $S_2C\delta$, V, TML_ε, and $TMLB'\delta$.

[3] 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 3.1.3.

3.1.2.2 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 definition 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 3.1.2.1, 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 XI 3-1 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 combinations 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

---

[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 XI 3-1. 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.

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 XI 3-2 and XI 3-3 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 dependencies 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

TABLE XI 3-2. 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%	100%[a]
$10^{-3} \leq Q_U < 10^{-2}$	7	32%	
$10^{-2} \leq Q_U < 10^{-1}$	8	36%	

(a) Percentage of systems whose unavailability $\geq 10^{-4}$.

TABLE XI 3-3. 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%	
$10^{-3} \leq Q_U < 10^{-2}$	5	28%	89%[a]
$10^{-2} \leq Q_U < 10^{-1}$	2	11%	
$10^{-1} \leq Q_U < 10^{0}$	2	11%	

(a) Percentage of systems whose unavailability $\geq 10^{-4}$.

TABLE XI 3-4. 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.

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

[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 XI 3-5. 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.

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 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 XI 3-4 and 3-5 give a breakdown of the various contributions that were calculated for the system failure probabilities categorized as to hardware, test and maintenance, human,

[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.

and common mode, where common mode also includes human-caused dependencies.[1] 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.

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 the combinations, the fault tree was then reevaluated to determine the change in the system failure probability.[2]

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 analyses 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. 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.

---

[1] The contributions are based on the point value calculations given in Appendix II.

[2] 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.

3.1.2.3 Overview of the Handling of Common Mode Failures[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) (XI 3-1)

and

$$P_{IE} \times P_{SF} \times P_{CF} \times P_{CFM} \times P_{WC} \times P_{PD}$$

(for transients). (XI 3-2)

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 Event Tree

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

[1] In this section, the symbol P represents probability and the various subscripts are defined as follows: IE = initiating event; SF = system failure; CPM = containment failure modes; WC = weather conditions; PD = population density; CF = component failure.

(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 XI 3-1 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 XI 3-1, 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:

$$
\begin{aligned}
P_{IE} &\simeq 10^{-3} \\
P_{SF} &\simeq 10^{-2} \\
P_{CFM} &\simeq 10^{-1} \\
P_{WC} &\simeq 10^{-1} \\
P_{PD} &\simeq \underline{10^{-2}} \\
&\qquad 10^{-9}
\end{aligned}
$$

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 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:

$$
\begin{aligned}
P_{IE} &\simeq 10 \\
P_{SF} &\simeq 10^{-4} \\
P_{CF} &\simeq 10^{-2} \\
P_{CFM} &\simeq 10^{-1} \\
P_{WC} &\simeq 10^{-1} \\
P_{PD} &\simeq \underline{10^{-2}} \\
&\qquad 10^{-9}
\end{aligned}
$$

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 $P_{SF} \times P_{CF} \simeq 10^{-6}$. 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.

3.1.3 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.[2] 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,[3] 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 ($\sim$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

---

[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.

[2] 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.

[3] During the refueling operation, a single fuel assembly is in transit between the reactor vessel and the spent fuel storage pool.

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 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.

3.1.3.1 Potential Accidents Involving the Reactor Core

Figure XI 3-6 shows the matrix of potential accidents considered for the reactor core. Line 1 shows those accidents that 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 XI 3-6, 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

[1] WASH-1400 only examined potential shipping cask accidents that could occur at reactor sites. It did not consider transportation accidents.

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 3.1.1 and 3.1.2 of this appendix 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.

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 1×10^{-5} per reactor-year and would not represent a major contribution to the overall likelihood of core melt.[3]

b. Figure XI 3-6, 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. XI 3-6 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. XI 3-6.

The general approach[4] 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

---

[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] The analysis performed to support this conclusion is described in section 3.2 of this appendix and is applicable only to the Browns Ferry plant. Additional work in the future to develop a more generally applicable model for handling the contribution of large electrical fires to risk assessments would be useful.

[4] See USNRC Regulations 10CFR50, Appendix A, General Design Criteria for Nuclear Power Plants.

10^{-9} to 10^{-8} per reactor-year.[1] 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 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. XI 3-6 indicate that external events are not expected to have a major impact on the risks associated with reactors.[2]

c. Figure XI 3-6, 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 16 of this appendix and section 5.4.6 of the Main Report discuss this matter in greater detail.

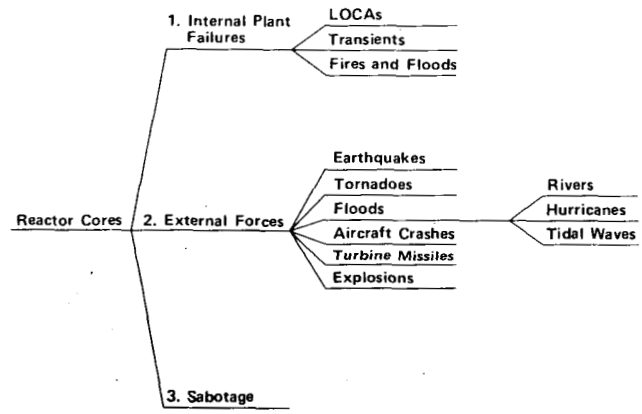


Figure XI 3-6. Coverage of Potential Accidents in Reactor Cores

[1] See Appendix III, section 6.2, and Main Report, section 5.4.4, for a fuller discussion of this matter.

[2] 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.

3.1.3.2 Potential Accidents Involving the Spent Fuel Pool.

Figure XI 3-7 shows the matrix of potential accidents considered for the spent fuel pool. As in Fig. XI 3-6, 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 XI 3-7, 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;[1] or an increase in 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 XI 3-7, Line 2, External Forces

As previously noted in section 3.1.3.1, 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 3.1.3.1. 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

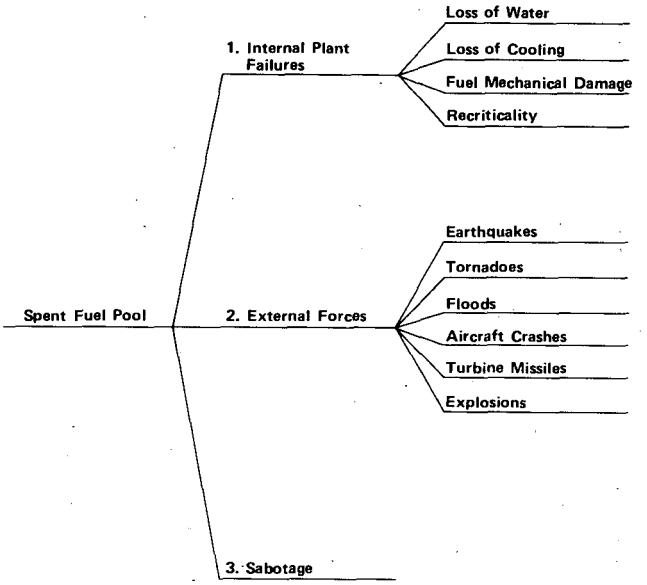


Figure. XI 3-7. Coverage of Potential Accidents Involving the Spent Fuel Pool

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 XI 3-7, Line 3, Sabotage

See section 3.1.3.1.c.

3.1.4 THE HANDLING OF FAILURE RATE DATA IN OVERALL RISK ASSESSMENT

The study received several comments on the adequacy of component failure rate data used for quantifying the event trees and fault trees. The comments questioned the basis for the data and the general random-variable, or range, approach used for the data treatment. This section presents an overview of the

[1] 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.

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)[1] 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.[2]

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:[3]

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)

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

---

[1] Section 14 of this appendix contains a further discussion of the treatment of human failures.

[2] In statistical terminology, the system probabilities were thus not strict probabilities but estimators.

[3] Appendix III gives a complete tabulation of the 77 sources used.

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 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

---

[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.

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 realistic and more meaningful. This method was applied to human error and 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.

3.1.5 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. Several comments requested amplification of the basic ideas behind event tree modeling and the methods of using fault trees in conjunction with event trees. This section discusses the basic logic and set-theory concepts of event trees and the use of fault trees in event tree models.

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.

---

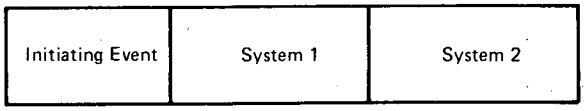
[1] In essence, this is analogous to treating the data as a set of samples from a statistical population on which a statistical and probabilistic analysis can be performed.

[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.

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.")

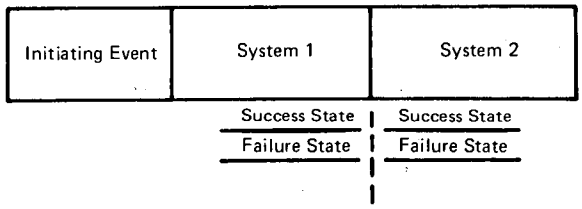


Example 1. Event Tree Heading

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.



Example 2. System State Definitions for System 1 and System 2

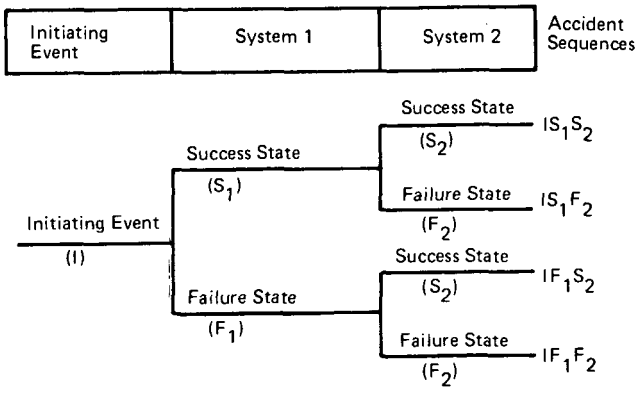
Appendix I, section 2, discusses in some detail the definitions of system success and failure states used in the study as well as their rationale. Since the system state definitions constitute one of the most significant parts of event tree methodology, certain general points will be noted during the 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

[1] In areas of uncertainty, potential success states that cannot be clearly demonstrated to be successful are assigned to the 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.



Example 3. Illustration of Event Tree Branching

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 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

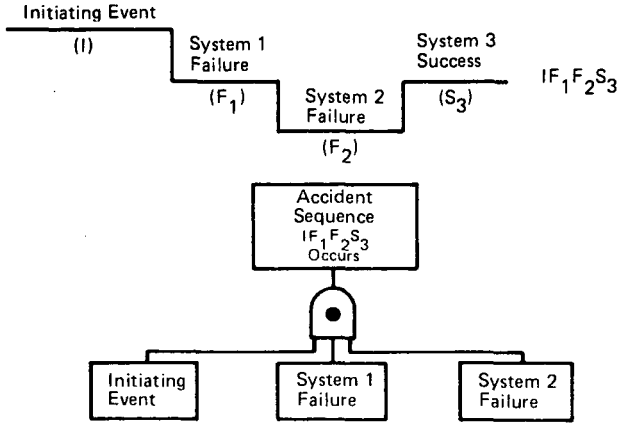
endeavor (How many competent jobs are done by incompetent people?). The Reactor Safety Study tried to obtain the most competent people in employing the services of 12 skilled fault tree analysts. These fault tree analysts worked closely with the system to gain an intimate knowledge of its workings. Detailed 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).



Example 4. An Accident Sequence and the Associated Fault Tree Construction

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.

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 quanitative 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.

3.2 SPECIFIC COMMENTS ON METHODOLOGY

The general comments received concerning the adequacy and utility of the WASH-1400 methodology were combined with other comments of a similarly broad nature and have been discussed in the preceding section 3.1. However, the study received a number of specific comments that require a response in kind. These are presented below.

COMMENT 3.2.1

The recent fire at the Browns Ferry plant, an example of a common mode failure that disabled a number of systems of two power reactors simultaneously, emphasizes the need for a thorough examination of common mode failures.

(U.S. Environmental Protection Agency)

RESPONSE

An extensive discussion of the overall methodology used in the analysis of common mode failures by the Reactor Safety Study is provided in section 3.1 of this appendix to respond to the many comments received on this subject. The reader is referred to that section for a better exposition of the methodology than was provided in the draft report.

However, since the draft report did not specifically address the potential risks that could be associated with large electrical fires, this response provides some further discussion of that area as well as a specific analysis of the impact of the Browns Ferry fire on the probability of a core melt accident.

The potential for large electric fires was considered qualitatively by the study in the course of its accident analyses. The study concluded at that time that the start of a fire in or near the cable spreading area was a relatively low probability event in comparison

[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.

with some other types of events considered in the study, that the use of fire prevention and firefighting techniques would limit the extent of a fire, and that even if a large fire occurred, it would be unlikely, because of such design features as cable separation, to cause a large release of radioactivity.

To check the validity of its qualitative judgment, the study has made a quantitative assessment of the potential for the Browns Ferry fire to have caused a significant release of radioactivity. The results of this analysis indicate that the potential for a core melt accident as a result of the fire is estimated to be about 20% of that obtained from all other causes analyzed in WASH-1400. Since this value is within the band of uncertainty of the predictions made in WASH-1400, it can be said that, if this fire is typical of the possible gamut of large electrical fires at nuclear power plants, the Browns Ferry fire does not affect the validity of the overall WASH-1400 risk assessment. Furthermore, a lesson that emerges clearly from the examination of the fire that occurred is that rather straight-forward measures, such as may already exist at other nuclear plants, can improve fire prevention and firefighting capability and can significantly reduce the likelihood of a potential core melt accident that might result from a large fire.

It should be recognized that the analysis of the fire at Browns Ferry necessarily concerns itself with the specific sequence of events that actually occurred. Thus the conclusion stated above (i.e., the fire that occurred does not constitute a major contributor to the risk of a core melt accident) may be of somewhat limited applicability. It would be useful to pursue the collection and analysis of data associated with fires as well as the development of a risk model for the treatment of fires.

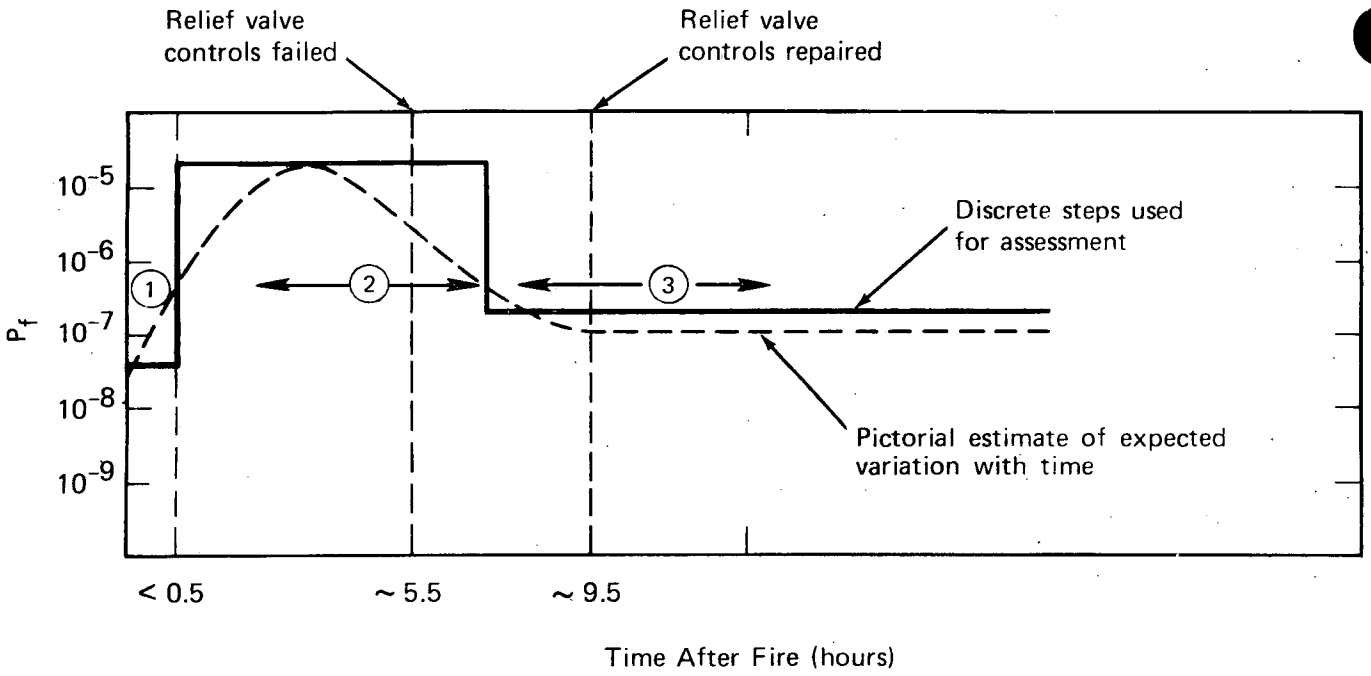
The specific analysis of the fire was performed for plant No. 1 since the equipment damage in plant No. 2 was much less extensive; thus the analysis for plant No. 1 bounds the probability of core melt at Browns Ferry as a result of the fire.

An examination of the course of events during the fire indicates that there were three time periods (hereafter called phases 1, 2, and 3) of interest in analyzing the likelihood of a large release of radioactivity.[1] Figure XI 3-8 indicates the times of interest and the predicted probabilities of core melt. Once the reactor was shut down, the situation required the removal of decay heat, as described in the transient event tree in section 4.3.2 of Appendix I. Since the normally used decay heat removal system had been made inoperable by the fire, it was necessary to rely on alternative means for performing this function. In phase 3, with the ability to open and close the remotely actuated reactor vessel relief valves from the control room, decay heat could be removed from the core by discharging steam (and its associated heat) from the reactor vessel to the containment vapor suppression pool. At the same time water could be pumped (at relatively low pressures of 350 psig since opening of the relief valves could maintain the vessel pressure at low levels) from various storage areas into the reactor vessel to ensure that the fuel remained covered. A significant number of pumps, each of which could accomplish this function, were available. A large amount of equipment was available in both phases 1 and 3.

In phase 2, decay heat could be removed either by pumping water at relatively high pressures (from >350 psig up to about 1000 psig) and having safety valves open to remove steam and its associated heat or by RV depressurization. As indicated later, some normally operating equipment (the control rod drive pump) was available to add water at high pressure, but it required augmentation by backup equipment, some of which required significant times to activate, in order to ensure that an adequate level of water was maintained in the vessel. Although the relief valve control failed at approximately 5.5 hours after the fire and was repaired in approximately 4 hours, the analysis of phase 2 also considered potential variations that could have occurred both in the time of failure and in the time to repair the control.

---

[1]The course of events that occurred during the fire is described in the following reference: U.S. NRC Office of Inspection and Enforcement, Region II, report of Tennessee Valley Authority Browns Ferry Unit 1 and Unit 2, #50-259/75-1 and #50-260/75-1, "Fire in the Cable Spreading Area and Reactor Building on March 22, 1975," of July 25, 1975.



P_f = Total estimated probability of fire-caused core melt at Browns Ferry.

(1) = Phase 1 of the fire, during which significant amounts of equipment were available for adding water to reactor vessel.

(2) = Phase 2 of the fire, during which the controls for the reactor vessel relief valves were or could have been failed, thus requiring the addition of water to the vessel at higher pressures (up to approximately 1000 psig).

(3) = Phase 3 of the fire, during which the controls for the reactor vessel relief valves were or could have been repaired, thus requiring only low-pressure water addition.

Fig. XI 3-8. Predicted Probability of Core Melt versus Time During the Browns Ferry Fire.

Attachment 1 consists of the logic trees for phases 2 and 3 (Figs. 1 and 2, respectively), the list of potentially available equipment for phases 2, and 3, and the evaluation of the trees. It is noted that these logic trees are in summary form and do not depict all repair substeps discussed herein. Evaluation of the logic trees yields conservatively estimated value of 1.0×10^{-5} and 4.0×10^{-7} for phases 2 and 3, respectively. An evaluation of phase 1 would yield results similar to those for phase 3.

Attachment 1 to Section 3.2.1

Analysis of the Browns Ferry Fire

PHASE 2

FAILURE POSSIBILITIES FOR PHASE 2

During phase 2, had the control system for all 11 relief valves been inoperable, the single operating control rod drive (CRD) pump would have been incapable of maintaining an adequate level of water in the core at high pressures.[1] Examination of the ways in which the CRD flow could have been augmented revealed that the high-pressure makeup sources listed below were, to varying degrees, viable options for this purpose.

High-Pressure Makeup Sources

RCIC - The controls needed to open the reactor core isolation cooling system valves were disabled by the fire, obviating the ability to use decay heat steam from the core to operate the steam-turbine-driven pump. However, the RCIC delivery could have been restored by using steam from the on-site auxiliary boiler. Consideration of the steps involved to provide steam to the RCIC revealed that its operation could have been restored within the available 2-hour repair time window. (These repair actions were in fact under way.)

HPIS - The high-pressure injection system was also disabled by the fire, and repair actions quite similar to those for the RCIC system would have been needed. Repair of this system involved the installation of a large spool piece connection under difficult access conditions. Furthermore, the HPIS repairs had, in fact, not been made within about 26 hours after the start of the fire. For these reasons, the HPIS option was taken as not being a very viable option (i.e., a failure probability of 1.0 was assumed).

Other Possible High-Pressure Makeup Sources

SLC - The standby liquid control system was without electric power for several hours into the fire; however, this system could have been energized by repair action if necessary. The SLC consisted of several positive displacement pumps (each with a capacity of about 56 gpm) that could have been placed into operation to satisfactorily augment the CRD pump flow.

CRD Spare Pump and Pump from Plant No. 2 - The use of an additional CRD pump could not have satisfactorily augmented the existing CRD flow by providing enough incremental flow to keep the vessel inventory at suitable levels. Thus, these are not shown on the logic tree as a viable option.

CRD Bypass Flow - Opening of a bypass line in the CRD system would have satisfactorily augmented the existing CRD flow by redirecting an incremental flow to the reactor vessel, which would have approximately doubled the existing CRD flow.

EVALUATION OF PHASE 2 LOGIC TREE

Best-Estimate Evaluation

For the quantification, the event symbols will be used as shown on the tree (Fig. 1) and P_2 will denote the probability of the event during phase 2.[2]

The availability of a large number of plant personnel during the course of the fire and time windows available provide the basis for the assumption that repairs could be performed simultaneously in several areas when multiple

---

[1] In actuality, a single CRD pump was operating in this interval, and the remaining 4 of 11 relief valves allowed the plant operator to manually depressurize the reactor coolant system to a pressure level (<350 psi) where the low-pressure condensate pump could be used to augment the CRD makeup capacity.

[2] Exponential outage modeling is used for repair lasting longer than the critical maximum time, as described in section 3.5.3 of Appendix II.

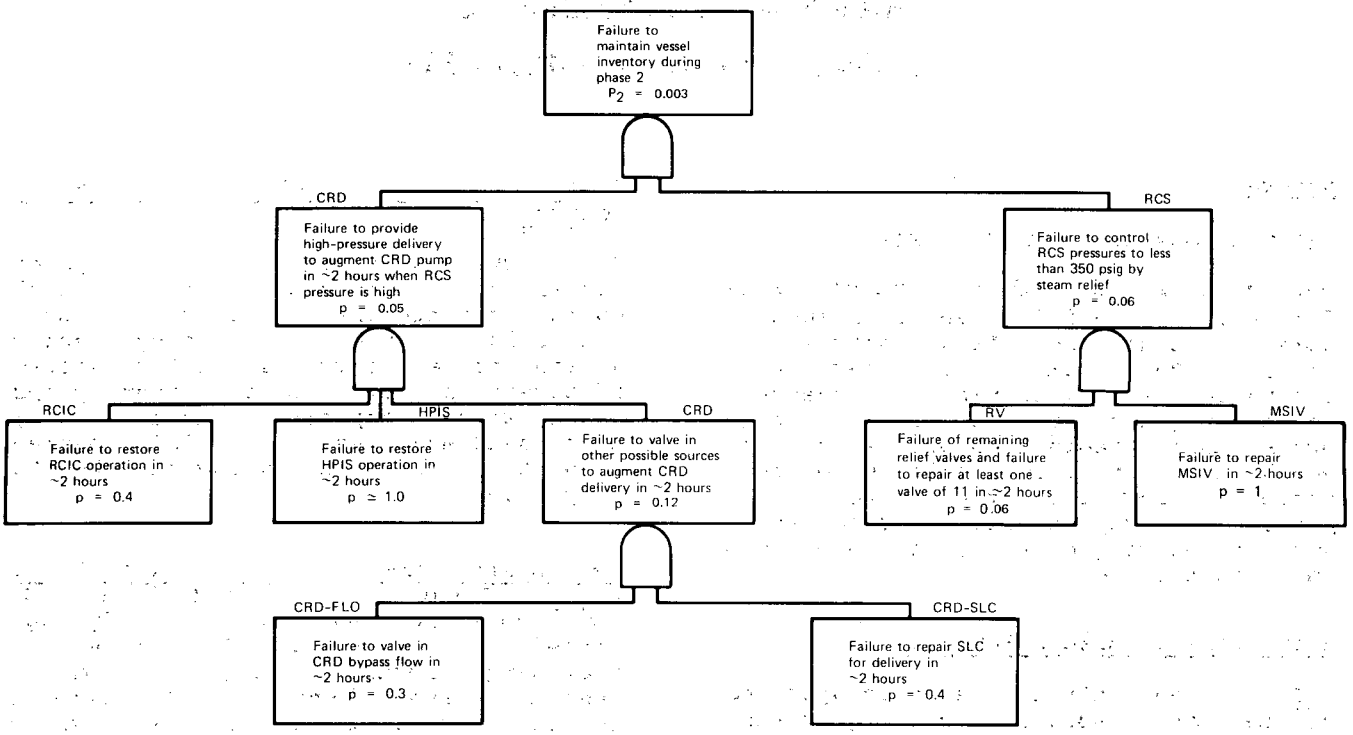


Figure 1. Failure Possibilities for Time Less than 5.5 Hours After Fire Start.

failures occur. Therefore, from the straightforward tree logic, the probability of inability to maintain vessel inventory, P_2, can be expressed as[1,2]

$$P_2 = P(RCIC) \times P(HPIS) \times P(CRD\text{-}FLO) \times P(CRD\text{-}SLC) \times P(RV) \times P(MSIV).$$

Using the above equation, a best-estimate calculation can be performed for the actual incident, and then sensitivity studies can be made to establish bounding values. Since the HPIS and MSIV were still unavailable approximately 26 hours into the actual incident, they are taken as not being very viable options; that is, for the best-estimate calculations, P(HPIS) ≃ 1 and P(MSIV) ≃ 1. The probability P_2 therefore becomes

$$P_2 = P(RCIC) \times P(CRD\text{-}FLO) \times P(CRD\text{-}SLC) \times P(RV).$$

The actual repair of the SLC required approximately 3.5 hours.[3] However, a value of 2.5 hours is used as the best estimate of the repair time because it has been estimated that if the SLC had been required, it could have been repaired in about 1 hour.[4] Also, the

[1] Symbols refer to events as identified on the fault trees.

[2] The use of Boolean algebra in quantification is extensively discussed in Appendix II.

[3] U.S. NRC Office of Inspection and Enforcement, Region II, report of Tennessee Valley Authority Browns Ferry Unit 1 and 2, #50-259/75-1 and #50-260/75-1, "Fire in the Cable Spreading Area and Reactor Building on March 22, 1975," July 25, 1975.

[4] Statement by Benard C. Rushe, Director of Office of Nuclear Reactor Regulation, U.S. NRC, Before the Joint Committee on Atomic Energy, September 16, 1975.

relief valves were observed to fail at approximately 5.5 hours, and the repair required 3 hours and 50 minutes (3.8 hours). These two values will be used as the best estimate of the mean failure time and repair time, respectively. (The calculations are thus conditional on these values being observed and used.)

Using the above values, the two probabilities (PCRD-SLC) and P(RV) are evaluated as[1]

$$P(\text{CRD-SLC}) = \exp(-2/2.5) = 0.4,$$

where a 2-hour time is available before coolant falls below acceptable limits.

$$P(\text{RV}) = [1 - \exp(-5.5/5.5)]\ \exp(-2/3.8)\ (\exp\{-2[(\ln 2)/0.5]\} + 0.1) = 0.06,$$

where 5.5 hours is used for the time possible for failure and a 2-hour outage time is again used. The relief valve failure, RV, consists of failure of four relief valves remaining without their repair, failure to repair those valves initially failed or failure of the accumulators for the valve controls.

Since repair times were not observed for the RCIC failure (i.e., restoration of RCIC operation), the CRD-FLO failure (i.e., valving in the CRD bypass flow), these repair times were estimated. Based on the operations involved, the median repair times are estimated as follows:

System	Median Repair Time (hours)
RCIC	∿1.5
CRD-FLO	∿1.0

The restoration of the RCIC operation involves disconnecting the electrical leads, connecting the spool piece, and developing sufficient steam from the auxiliary boiler. The limiting items involve the spool piece connection and the steam development. The median time for performing these operations is estimated to be 1.5 hours under efficient operator utilization.

The CRD-FLO involves a valving operation, the estimated median times being 1.0 hour.

The above median repair times account for response and diagnosis times as well as actual repair. Sensitivity studies are performed below to investigate the effects of different repair times on these and the other failures.

Using the above median estimates and transforming to the mean repair times required for the exponential outage equations, one obtains the following failure probabilities:

$$P(\text{RCIC}) = \exp\{-2[(\ln 2)/1.5]\} = 0.4,$$

$$P(\text{CRD-FLO}) = \exp\{-2[(\ln 2)/1.0]\} = 0.3,$$

Therefore using the above probabilities for CRD-SLC, RV, RCIC, and CRD-FLO, the probability of failure to maintain vessel inventory is then

$$P_2 = 0.4 \times 0.06 \times 0.4 \times 0.3 = 0.003,$$

or approximately one in 300, given the fire occurrence.

Since approximately 200 reactor-years of experience exist, the probability of a fire occurrence is estimated to be 1/200, or 5×10^{-3} per reactor-year. Multiplying 0.003 by 5×10^{-3} then gives the (unconditional) probability of core melt from fire occurrences per reactor-year:

$$P_{F2}\ \text{core melt} = 0.003 \times 5 \times 10^{-3} = 1 \times 10^{-5}\ \text{per reactor-year.}$$

Sensitivity Evaluations

If the previously used median repair times for the RCIC, CRD-FLO and RV events are increased by 50% (i.e., the previous median values are multiplied by 1.5), then the following results are obtained:

[1] Results are rounded to one significant figure in this section.

$$P(RCIC) = 0.5;$$

$$P(CRD\text{-}FLO) = 0.4;$$

$$P(RV) = 0.1;$$

$$P_2 = 0.01;$$

and

$$P_{F2} \text{ core melt} = 5 \times 10^{-5}$$

per reactor-year.

Scaling the median times down by the same factor (1.5) gives the following lower bound values:

$$P(RCIC) = 0.3;$$

$$P(CRD\text{-}FLO) = 0.1;$$

$$P(RV) = 0.04;$$

$$P_2 = 0.0004;$$

and

$$P_{F2} \text{ core melt} = 2 \times 10^{-6}$$

per reactor-year.

The above values for the P_2 event and the occurrence of P_{F2} core melt (per reactor-year) can be taken as rough bounds on the best-estimate values computed in the preceding section.

PHASE 3

FAILURE POSSIBILITIES FOR PHASE 3

The Phase 3 structure logic presented in Fig. 2 involves essentially the same equipment as used in Phase 2, except that the flow required to maintain acceptable water level can be met by the operating CRD pump plus a number of alternative actions to augment its flow. As noted above, even if the operating CRD pump failed, the time window available for restoration of damaged equipment was estimated to be between 3 and 4 hours because the level of decay heat was diminished. These potential failures were considered in the quantification shown in Fig. 2.

EVALUATION OF PHASE 3 LOGIC TREE

Best Estimate Evaluations

The analysis is similar to that used for times shorter than 5.5 hours. The event symbols are shown on Fig. 2, which depicts the logic for times longer than 5.5 hours. (The tree logic shows the more significant contributors.) Since the logic is a bit more involved, the quantification will proceed from the bottom of the tree to the top. A 3.5-hour maximum outage time will be used in the calculations. For the CRD failure,

$$P(CRD) = (P(CRD\ 1) + P(CRD\ 2),$$

where again the event PUMP denotes both failure to use the spare pump and the plant No. 2 pump. Using the pump data in Appendix III and the previous 0.5 median repair time for the PUMP event,

$$P(CRD\ 1) = [1 - \exp(-1 \times 10^{-3} \times 24)]$$
$$\exp(-3.5/7)$$
$$\exp\{-3.5[(\ln 2)/0.5]\}$$
$$= 1 \times 10^{-4},$$

where a 1×10^{-3} per hour failure rate is used for the pump to account for possible degradation and a 7-hour repair time is used for pump repair.[1] Using the data in the previous section for the SLC failure and the CRD bypass failure, and using the observed repair time of approximately 6.1 hours for the steam drain line valves P(CRD 2) becomes

$$P(CRD\ 2) = \exp(-3.5/6.5)\ \exp(-3.5/2.5)$$
$$\exp(-3.5/6.5)\ \exp(-3.5/2.5)$$
$$\exp\{-3.5[(\ln 2)/1.0]\}$$
$$= 1 \times 10^{-2}.$$

Therefore

$$P(CRD) = 1 \times 10^{-4} + 1 \times 10^{-2}$$
$$= 1 \times 10^{-2}.$$

As in previous calculations, the HPIS event is not taken as a very viable option [P(HPIS) ≃ 1]. Using a 1.5-hour median time for the RCIC, as before,

[1] Section 5 of Appendix III.

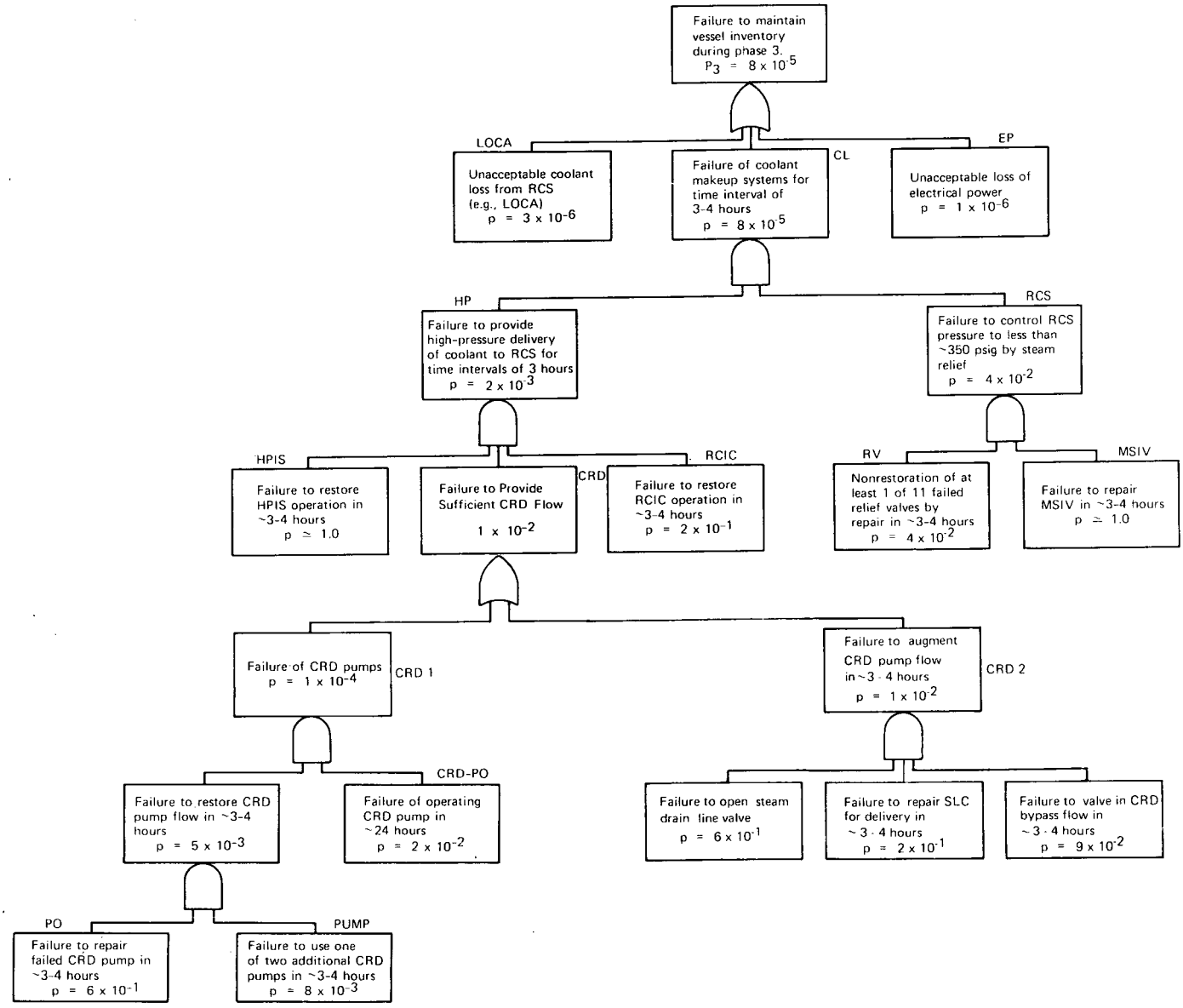


Figure 2. Failure Possibilities for Time Greater Than 5.5 Hours After Fire Start. (Note: Period of time actually considered for analysis purposes was about 1 day after fire.)

$P(RCIC) = \exp[-3.5\ (\ln(2)/1.5)]$

$= 2 \times 10^{-1}.$

Therefore

$P(HP) = P(CRD) \times P(RCIC) = 2 \times 10^{-3}.$

In the RCS event, the MSIV is again not taken as a very viable option, and hence

$P(RCS) = P(RV) = \exp(-3.5/3.8),$

$\times(\exp\{-3.5[(\ln 2)/0.5]\}$

$+ 0.1)$

or

$P(RCS) = 4 \times 10^{-2},$

using similar logic as in Phase 2. The probability for the CL event therefore becomes

$$P(CL) = P(HP) \times P(RCS) = 8 \times 10^{-5}.$$

The LOCA contribution to the P_3 top event (using the linear approximation to the exponential) is

$$P(LOCA) = 10^{-3} \times 24/8760 = 3 \times 10^{-6},$$

where a small-pipe-rupture number of 1×10^{-3} per year is used.

Finally, the electric power contribution is (again using the linear exponential approximation)

$$P(EP) = 2 \times 10^{-5} \times 24 \times .2 \times 1 \times 10^{-2}$$
$$= 3 \times 10^{-6},$$

where the failure rate for loss of offsite power is taken as 2×10^{-5} per hour and a 0.2 probability is taken for the critical outage duration.[1] A probability of 10^{-2} per demand is used for the unavailability of the diesels.[1]

The total probability for the top event, P_3, given the fire occurrence, is

$$P_3 = P(CL) + P(LOCA) + P(EP)$$
$$= 8 \times 10^{-5} + 3 \times 10^{-6} + 1 \times 10^{-6}$$
$$= 8 \times 10^{-5}.$$

The unconditional reactor-year probability is obtained by multiplying by 5×10^{-3}, or

$$P_{F3} \text{ core melt} = 4 \times 10^{-7} \text{ per reactor-year.}$$

The error spread on the above values would be approximately a factor of 10 in either direction and arises principally from the pump failure rate error and median repair time errors. (The pump failure rate error is given in Appendix III, and the median repair time errors were investigated in the previous calculation.)

End of Attachment 1

COMMENT 3.2.2

With regard to PWR reactor vessel rupture, Appendix I, section 4.1.4, it is not clear how the polar crane presents an effective missile barrier for the entire upper portion of the containment.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

The presence of a polar crane, such as is used in all PWR reactors, serves to protect the integrity of the containment against the impact of upward-bound missiles occurring from failures in the upper region of the reactor vessel.

Such missiles could arise from potential failures of the vessel in its upper region (specifically failures of the head bolts or failure in a region under the reactor vessel flange that supports the core). Initial analyses using conservative assumptions as to the acquired momentum of the head and/or core, but excluding the presence of the crane, revealed that the momentum would be such that a breach of containment integrity could not be ruled out. However, additional analyses, taking into account the presence of the 200-ton crane directly over the centerline of the reactor vessel and the possible trajectories of the vessel missiles, revealed that the crane would prevent such potential missiles from impacting on the containment building, and thus they could not cause failure of the building. Since the crane is always present over the vessel centerline, the study concluded that the probability of such missiles leading to a breach of the containment is negligibly small.

COMMENT 3.2.3

In section 4.1.5 of Appendix I, the reason for not considering rupture of

---

[1] Section 6.3.3 of Appendix III.

steam generator tubes and subsequent overpressurization of the secondary system with potential for rupture outside the containment should be stated.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

The impact of steam generator tube ruptures was assessed, and the potential for the overpressurization and rupture of the secondary system outside the containment was considered. The specific sequence postulated by this comment, though not explicitly addressed in section 4.1.5 of Appendix I, is covered in section 4.1.6 "PWR RCS Ruptures into Interfacing Systems." In examining the potential for steam generator tube failure to overpressurize the secondary system, one must consider that operation of the safety/relief valves provided on the steam generator would preclude this event. As discussed in sections 4.3.1 and 4.3.2 of Appendix V, the probability of failure of these secondary steam relief valves is negligibly small.

COMMENT 3.2.4

In section 4.2.1 of Appendix I, it is not obvious why the situation of automatic trip failure occurring with loss of electric power sequence was eliminated from consideration.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

It is correct that the BWR LOCA event trees do not show a failure path that includes failure of electric power and failure of the reactor protection system. This path was eliminated because the loss of electric power de-energizes the power contactors in the reactor protective system; this automatically initiates the signal for the control rods to insert. The failure probability of this insertion is less than 10^{-5} per event. Since the loss of electric power can lead to core melt whether or not scram occurs, a failure to scram would only affect the timing of the core melt (i.e., it could occur approximately 0.5 to 1 hour sooner). This earlier melt would result in only a minor increase in the fission products released and therefore makes no significant change in the consequences of this accident sequence.

COMMENT 3.2.5

In the LOCA functional event tree development in section 2 of Appendix I (relative to the footnote about post accident hydrogen generation) it appears that the containment building purge system has a probability of failure which is not acknowledged.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

The discussions that develop the LOCA functional event tree indicate that the operability of the PWR hydrogen control systems did not affect the overall assessment of risks in a significant way. In situations where the core does not melt, the rate of hydrogen generation by radiolysis would be low, and it would take weeks for the hydrogen concentration to reach flammable limits in the containment. Thus, if hydrogen purge systems were to fail, there would be a high chance of repair in this interval. Furthermore, the radioactivity release would be small during a hydrogen purge and the magnitude of release would be covered by the PWR sequences A and Aβ; these did not contribute significantly to the accident risks.

COMMENT 3.2.6

Containment failure occurring due to overpressure several hours after core melt is mentioned, but no credit is taken for measures that could be taken to prevent overpressurization.

(General Electric Co.)

RESPONSE

The analyses performed in WASH-1400 suggest that controlled containment venting or other means of preventing containment failure due to overpressure by steam and noncondensable gases might potentially provide some reduction in the risks associated with reactor accidents. However, no credit was given for operator action in this regard because it would entail a violation of existing procedures. Furthermore, the study sought to determine if venting could be effective in the case of a large LOCA in a BWR since there are both drywell and wetwell vents. These vents have an effective venting size of a 1 inch diameter hole, and only one vent can be operated at a time. As stated in section 3.3.2 of Appendix VIII, "small containment iso-

lation failures, i.e., equivalent to a 1-in.-diam holes or less, will not preclude containment failure by overpressurization." Therefore, controlled venting to prevent containment overpressure failures did not appear to be a viable option in the plant analyzed.

COMMENT 3.2.7

Comments were received that questioned the smoothing technique used in combining the event tree sequences to determine the probability of a given release category. These comments questioned the theoretical basis for smoothing, and most indicated an opinion that the use of smoothing introduced undue conservatism.

(U.S. Environmental Protection Agency;
General Electric Co.;
Westinghouse Electric Corp.;
Amory Lovins)

RESPONSE

As described in section 3.1 of this appendix and section 4.1.2 of Appendix V, the smoothing technique is used to account for the possible variability in the magnitude of radioactive releases from a particular accident sequence. Because of this variability, an accident sequence that is assigned to a particular release category has some possibility of falling into adjacent categories. The smoothing thus accounted for the chance of this miscategorization which had not been included in selecting the particular values of release magnitudes.

While it is true that the use of smoothing may introduce some conservatism, the values chosen were based on the engineering judgment of those involved in the calculation of release magnitudes. The elimination of smoothing is clearly unwarranted because the real variations possible in the physical processes affecting radioactive release magnitudes would have been omitted from consideration.

COMMENT 3.2.8

One comment referenced an unsuccessful application of reliability techniques to the analysis of the ignitor of a Skybolt missile because of the presence of flaws induced by welding.

(Union of Concerned Scientists)

RESPONSE

It is always important to verify that the population of collected failure rates is applicable to the particular situation under analysis. If the populations for failure data had contained welding-related failures, then the failure rate range from that population (and not the point value) would have encompassed the pertinent situation. One cannot generally use point values and treat them as being exact since there will always be variabilities and uncertainties. This is why the study believes that the random-variable treatment represents a realistic and believable approach.

COMMENT 3.2.9

There was a comment questioning the maintenance treatment used in the study's fault tree quantifications. For a doubly redundant system, the study obtained the maintenance contribution by multiplying the maintenance downtime contribution of one leg by the unavailability of the other redundant leg. An additional detection factor was suggested as being required in this multiplication which would reduce the overall maintenance contribution. The study's use of a given maintenance frequency, independent of the system unavailability, was also questioned.

(General Electric Co.)

RESPONSE

The unavailability contribution that the study used to multiply the downtime contribution was the undetected contribution (i.e., the unavailability contribution due to those failures that would not be detected before or during the maintenance act). In certain of the study's fault tree quantifications, the total unavailability was reduced by the detected contribution to obtain the applicable undetected contribution that was used in the multiplication.

The maintenance frequency used in the study did not apply to systems but to individual components. In general, these components consisted of pumps, valves, and other active components. From the maintenance data examined (section 5 of Appendix III) no significant differences were observed in the maintenance frequency, within the accuracies of the analysis.

COMMENT 3.2.10

Examples were given of actual incidents that involved several sequential human or equipment failures. The comment questioned the ability of the study to predict such events using the methodology employed in WASH-1400.

(Union of Concerned Scientists; The National Intervenors)

RESPONSE

In performing its assessment, the study reviewed not only the examples cited in the comment but also many other sources of pertinent data. The study's analyses were not meant to be taken out of context and extrapolated to different situations or different sequences. Sequential failures must be treated by sequential methods; alternatively, it is necessary to identify, by the use of methodology similar to that discussed in sections 3.1.2.1 and 3.1.2.2c of this appendix and in Appendix I, single based causes that govern the sequences of failures. In one instance cited, aging was used as an example of a common mode failure. It should be recognized that the study did not include extreme aging considerations since the applicability of its results is limited to only the next 5 years.

COMMENT 3.2.11

The risk calculation involved the assumption of double contingency on active components and single contingency on passive elements. Although the passive element assumption appears adequate, primarily because it is probably masked by active component failure, it is felt that the exact solution should be calculated for these cases. The assumption of double contingency on active components, however, probably results in overconservatism by a factor of at least 3. The experience in one major utility has been, that, for a typical series (parallel 30 component systems for an electric station with 16 successful paths) there is a 4 to 1 variation in calculation of the mean time between failures to carry out the mission in the conservative direction when the double contingency solution is compared to the exact calculation.

(Edison Electric Institute)

RESPONSE

Double contingency was not assumed; however, double failures were retained when they existed and consisted of active components.[1] The exact probability obtained by keeping all redundancies will be not lower but somewhat higher in comparison to the probabilities obtained by keeping only certain combinations). The effect will be small, however, if the dominant failure contributions have been identified.

COMMENT 3.2.12

The discussion in section 2.4 of Appendix II, volume 1, is unclear. The relation to regulatory single-failure criteria should be explained.

(Amory Lovins)

RESPONSE

The referenced discussion does not have any relationship with the Nuclear Regulatory Commission's single-failure criterion. The Nuclear Regulatory Commission's single-failure criterion is a design requirement imposed to achieve suitable redundancy in safety systems. The referenced discussion pertains only to the quantitative methods that were used in evaluating WASH-1400 fault trees.

COMMENT 3.2.13

A comment was received on the study's handling of certain common mode failures. An example was given of miscalibrating four parallel channels. Table III 3-5 in Appendix III was cited as giving three such failures out of a total of 303 failures, which was interpreted as yielding 10^{-2} for the miscalibration error (3/303). This was stated as being at odds with the tight coupling assessment used in Appendix III giving 3×10^{-5} or the loose assessment coupling assessment described in Appendix IV which the comment used to give 3×10^{-8}.[1] Another example was then given in which the study's methodology was purportedly used to obtain 10^{-20} for a sequence of seven triple common mode failures that actually occurred (E. P.

[1] In the above context, double contingency implies that any double active failure is assumed to fail the system. However, the fault trees used in the study determined which doubles would fail the system (i.e., the minimal cut sets) and only these, out of all the possible doubles, were included.

Eppler, "The ORR Emergency Cooling Failure," Nuclear Safety, Vol. 11, p. 323, July-August, 1970).

(Union of Concerned Scientists)

RESPONSE

First of all, the 10^{-2} probability obtained from Table III 3-5 is a relative probability; i.e., given that a failure has occurred, there is a 10^{-2} probability that it will involve the miscalibration of four channels. If the data in Table III 3-5 are used to obtain the absolute probabilities of the type computed in the study, then the 10^{-2} probability must be multiplied by the probability of a failure occurring. If, for example, one uses 10^{-3} (per demand) as an approximately general human error rate, then one obtains $10^{-3} \times 10^{-2}$, or 10^{-5} (per demand), for the approximate absolute miscalibration rate. Since Table III 3-5 has only gross data with regard to human errors, these data were used principally to check the study's assessment. The actual quantifications were performed using the methodology and data described in section 6.1 of Appendix III. The loose coupling methodology described in Appendix IV is only to be applied when there are no strong potential dependencies. The discussion in Appendix IV only gives the various kinds of techniques that can be used in common mode bounding and quantifications. The actual quantification, and the particular technique used, is given in the relevant fault tree quantification.

With regard to UCS's use of WASH-1400 methodology to obtain 10^{-20} for a sequence of seven triple failures, the study believes that the methodology cannot be used in this manner. As described in the discussion in section 3.1 of this appendix, the methodology, when correctly applied, is used to determine the significant contributors and failure causes. The application of the methodology in the study has identified that the significant contributors to the probability of reactor accidents involve only a small number of failure causes; i.e., single system failures that are dominated by single type failures within systems. When these exist, as they did in the study's applications, then the contribution from seven triple failures will necessarily be small and will not affect the results.

[1]The 3×10^{-5} value is the log-normal median of 10^{-3} and $10^{-3} \times 10^{-2} \times 10^{-1} \times 1$, where 10^{-3} is the individual miscalibration rate and 10^{-2} and 10^{-1} are the probabilities of additional miscalibrations. The 3×10^{-8} value is the log-normal median of 10^{-3} and 10^{-12}, where 10^{-12} is the probability of four independent miscalibrations.

Section 4
Consequence Model

4.1 INTRODUCTION

In its efforts to improve the computation of potential consequences, and as a result of the comments received, the study developed a new consequence model.[1] The principal objectives of this effort were to correct the errors in the old model, to make a more realistic and better justified prediction of doses and dose-response relationships, and to include the time variation of weather parameters. While a higher degree of realism was achieved in dosimetry and health effects predictions, the treatment of meteorological parameters resulted in a meteorological model that still appears to be significantly conservative. Table XI 4-1 summarizes the average and peak values of the consequences predicted by the consequence models used in the draft and final reports.

4.2 COMMENTS AND RESPONSES

A great many comments that were received indicated that the potential conse-

TABLE XI 4-1 CONSEQUENCE MODEL PREDICTED AVERAGE AND PEAK VALUES

Consequence	Draft Report	Final Report	Change Factor
	Average Values (per reactor year)		
Early Fatalities	5×10^{-4}	3×10^{-5}	x.06
Early Illness	1×10^{-3}	2×10^{-3}	x2
Thyroid Illness	7×10^{-2}	2×10^{-1}	x3
Latent Cancer Fatalities	3×10^{-3}	2×10^{-2}	x7
Genetic Effect	3×10^{-3}	4×10^{-3}	x1.3
Property Damage	$18,000	$20,000	x1
Relocation Area	NA	2×10^{-3} Mi^2	-
Decontamination Area	NA	3×10^{-2} Mi^2	-
	Peak Values ($\sim 10^{-9}$ per reactor year)		
Early Fatalities	2300	3300	x1.4
Early Illness	5600	45,000	x8
Thyroid Illness	2800/yr	8000/yr	x3
Latent Cancer Fatalities	110/yr	1500/yr	x14
Genetic Effects	106/yr	170/yr	x1.6
Property Damage	$6.2 billion	$14 billion	x2.3
Relocation Area	30 mi^2	290 mi^2	x10
Decontamination Area	400 mi^2	3200 mi^2	x8

[1] U.S. Environmental Protection Agency; U.S. AEC Regulatory Staff; American Physical Society Study Group on Reactor Safety; Resources for the Future, Inc.; Union of Concerned Scientists.

quences predicted in the draft report were too low. The principal comments and the actions taken in response to them are discussed in this section. The justification for all of the modeling changes discussed below are contained in Appendix VI.

COMMENT 4.1

The early fatalities predicted in the study have been underestimated by as much as a factor of 4. The arguments that the β dose to the gastrointestinal (GI) tract is not a contributor to fatalities are questionable, and the dose-response curve for acute fatalities may be in error. The evacuation model used is overly optimistic.

RESPONSE

The principal argument advanced for the presumed low estimate of early fatalities appears to be based on the idea that β doses to the GI tract will cause a larger number of fatalities than those estimated due to potential whole-body doses. While it is potentially possible for early fatalities to be caused by internal β irradiation of the GI tract, there is no history of such involvement except in cases where whole-body doses were already so high as to be lethal. It is estimated that a median lethal dose (LD_{50}) of about 5000 rads to the GI tract would cause such fatalities, as opposed to an LD_{50} of 510 rads for the whole-body dose. Since the ratio of whole-body dose to GI tract dose predicted in reactor accidents typically has a value of 1, it can be seen that GI tract fatalities will not contribute to the overall prediction of early fatalities from potential reactor accidents.

The dose-response curve for early fatalities in the draft report used an LD_{50} of 266 rads; the value in the final report has been increased to 510 rads.

A new evacuation model has been developed for use in the final report. It is based on a statistical reanalysis of the same data source[1] used in the draft report as opposed to an acceptance of the data analysis results presented in that source. The new model moves people at a slower rate than the old model.

COMMENT 4.2

Latent fatalities may be understated by as much as a factor of 25-50. The BEIR Report has been misinterpreted by a factor of about 2. The calculation did not include the effects of nonuniform doses to individual organs. Considerations pertinent to plutonium-241 were omitted.

RESPONSE

A new model for the calculation of latent cancer fatalities has been developed in which several significant parameter have been changed:

a. The model calculates the total man-rem based on individual organ exposures. The effect of this change was to approximately double the factor of 100 cancer fatalities per 1 million man-rem used in the draft report to about 200.

b. The dose-response curve for latent cancer fatalities was modified to depart from the linear hypothesis used in the BEIR report.[2] The basis for this modification was data that have become available since the publication of the BEIR Report and the advice of the study's medical consultants. The new approach uses a dose effectiveness factor which depends on the dose rate and dose magnitude; however it does not use a threshold dose value. The effect of this departure was to reduce the number of latent cancer fatalities predicted to about 100 per 1 million man-rem.

Additional isotopes, including plutonium-241 and other transuranics have been added to the consequence model. An error in the weathering half-life of cesium has been corrected, and this

---

[1] I. M. Hans and J. E. Sell, Evacuation Risks - An Evaluation, Office of Radiation Programs, National Environmental Research Center, Las Vegas, Environmental Protection Agency, EPA-520/6-74-002, June 1974.

[2] National Academy of Sciences - National Research Council, The Effects on the Populations of Exposure to Low Levels of Ionizing Radiation, Report of the Advisory Committee on the Biological Effects of Ionizing Radiations.

substantially increased the number of predicted latent cancer fatalities.

COMMENT 4.3

Genetic effects are understated by a factor as much as 25-60. The effects are predicted for only one generation as opposed to the net effect; this amounts to an underprediction of about a factor of 5.

RESPONSE

The estimates of genetic effects made by the study are based on the linear hypothesis used in the BEIR report and on the advice of the study's medical consultants. The draft report predicted only first-generation effects; the final report predicts first-generation and net effects.

COMMENT 4.4

Thyroid illness is understated by a factor of 4 due to the omission of effects on adults and the use of an incorrect dose-response factor for children.

RESPONSE

A new thyroid model has been developed based on the analysis of new data from clinical studies and that includes predictions of thyroid nodules and thyroid cancers. The new model incorporates effects on children and adults.

COMMENT 4.5

The property damage model is unsound. The population dose should not exceed 0.5 rem per year as opposed to the value of 5 rem per year used in the study. The resuspension of radioactivity deposited on the ground should be considered. The assumed decontamination efficiencies should be justified.

RESPONSE

An improved property damage model has been developed. It allows the accumulation of potential doses, calculated with cleanup of radioactivity, up to 10 rem over a 30-year period in rural areas and 25 rem over a 30-year period in suburban and urban areas without requiring the relocation of people. However, cleanup of radioactivity in such areas to reduce potential doses is included in the model.

The potential effects of the resuspension of radioactivity are included in the new model. The land decontamination factors are justified in Appendix K to Appendix VI. As noted earlier, the weathering half-life of cesium has been corrected.

COMMENT 4.6

The potential man-rem doses were truncated by computing doses out to only 500 miles.

RESPONSE

The new consequence model has been modified to eliminate this truncation. While the calculations are still only carried out to 500 miles, it is assumed that the residual radioactivity would be deposited on the ground in the last mesh point of the computer program and would thus contribute to the total man-rem doses. This procedure is justified because the principal contributor to doses at this distance would be cesium. Thus, calculating a ground dose from the ceisum component that would actually still be airborne as though it were deposited on the ground counts its total contribution to the potential man-rem dose.

COMMENT 4.7

The adequacy of the plume rise model is questionable.

RESPONSE

In the model used for the draft report, the heat generated by the radioactivity in the plume was allowed to heat the plume, thus causing the plume either to rise or to have enhanced vertical dispersion. The potential effects on plume rise of the sensible and latent heat that would be emitted from the containment along with the radioactivity were neglected.

In those potential accident sequences which involve steam explosions, the radioactive heating kept the plume off the ground for a considerable distance downwind of the reactor. In the ground-level releases, the heat was used to enhance vertical dispersion, but not to lift the plume off the ground.

A new plume rise model was developed for the final report. It uses the emitted sensible heat in a formation that causes the plume to rise. Depending on the emitted heat and the wind speed, the plume is permitted to rise off the

ground to varying heights; however the plume is not permitted to penetrate the inversion layer. This formulation is probably conservative because the altitude of the plume depends on the heat released and the latent heat (which can be quite high compared to the sensible heat) and radioactive heating are not used.

COMMENT 4.8

The consequence model does not include the time variation of weather parameters.

RESPONSE

The model has been modified to include the time variation of weather stability, wind speed, and rain. It does not include such factors as the effects of wind shear and changes in wind direction. The net effect of these changes was to make the meteorological model somewhat more conservative with regard to those consequences that are threshold dependent. These include early health effects, property damage, and land contamination.

2

Section 5
Probability of Accident Sequences

A number of comments that were received were directed toward the assessment of the probability of the various accident sequences identified. Each of these comments is discussed in this section.

Two of these comments, 5.1.1 and 5.2, identified errors in the draft report that resulted in changing the probabilities of two BWR transient sequences. In one case, the probability of failure of the BWR liquid poison injection system increased by a factor of 3. In the second, the probability of failure of the high pressure safety injection system and reactor core isolation cooling system to provide makeup water (event U) was decreased by a factor 4.

As a result of another comment questioning the use of large-LOCA analyses to predict the course of small-LOCA and transient events, detailed analyses were made of appropriate small-LOCA and transient event tree sequences. These analyses indicated that the probability of containment failure due to overpressure should be increased for certain sequences in the PWR. These analyses also suggested that sequence TWγ should be placed in BWR release category 3 as opposed to category 4 in the draft report.

In preparing the final report, the study also reviewed the assessments of all the principal sequences presented in the draft report. The review resulted in some small modifications to the assessed probabilities and indicated that sequence TWγ' had been inadvertently omitted from the compilation of BWR accident sequences. A number of the minor errors in sequence assignments were also corrected.

After adjustment, the overall probability of core melt of 6×10^{-5} per reactor-year predicted in the draft report decreased slightly to 5×10^{-5} per reactor-year. A detailed comparison of the adjusted probabilities of the various release categories to those originally assessed is presented in Table XI 5-1.

5.1 BWR TRANSIENT PROBABILITIES

There were several specific comments concerning the quantification of the BWR failure to scram probability. These are summarized below.

COMMENT 5.1.1

The credit taken for operator action in activating the liquid poison injection system appears to be incorrectly assessed. It does not appear reasonable to take credit for manual activation of the liquid poison injection system in the event of reactor protection system (RPS) failure based on the sequence and number of actions that must be taken by the operator. In view of these considerations, it is not clear why an operator error rate of 3×10^{-2} was used in WASH-1400.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

The matter under discussion deals with accident sequences initiated by transient events in which the reactor protection system fails to operate and the reactor must be made subcritical by alternative means. The principal alternative means involves manual activation of the liquid injection system by the plant operator. In the draft report, the probability of the operator failing to initiate poison injection had been assigned a value of 3×10^{-2} on the basis that, although only about 10 minutes were available for successful action, the action required the operator simply to press a button. However, a reexamination of the operating procedure for initiating system operation indicates that it requires the operator to use key lock switches, and the operating procedure suggests consultation with the plant supervisor before taking the action. The use of a value 10^{-1} for the probability of failure to initiate system operation would be more consistent with this situation than the previously assigned value of 3×10^{-2}.

A reassessment of this area as a result of the EPA comment resulted in a change in the value of 3×10^{-2} to 10^{-1} in the final report. This has resulted in an increase in the predicted probability of all sequences involving the failure of the reactor protection system by a factor of 3 as indicated in section 4.3.2

TABLE XI 5-1 COMPARISON OF THE PROBABILITIES OF THE VARIOUS RELEASE CATEGORIES ESTIMATED IN THE DRAFT AND FINAL REPORTS

Release Category		Probability per Reactor-Year	
Draft	Final	Draft	Final
PWR			
1	1	7×10^{-7}	9×10^{-7}
2	2	5×10^{-6}	8×10^{-6}
3	3	5×10^{-6}	4×10^{-6}
4	4	5×10^{-7}	5×10^{-7}
5	5	1×10^{-6}	7×10^{-7}
6	6	1×10^{-5}	6×10^{-6}
7	7	6×10^{-5}	4×10^{-5}
8	8	4×10^{-5}	4×10^{-5}
9	9	4×10^{-4}	4×10^{-4}
BWR			
1	1	9×10^{-7}	1×10^{-6}
2	2	2×10^{-6}	6×10^{-6}
3	3(a)	1×10^{-5}	2×10^{-5}
4		3×10^{-5}	
5	4	3×10^{-6}	2×10^{-6}
6	5	1×10^{-4}	1×10^{-4}

(a) BWR RELEASE CATEGORY 4 was combined with category 3 as a result of additional CORRAL calculations for small-LOCA and transient sequences and the reassignment of sequences to other release categories. After these changes were made, no significant differences existed between release categories 3 and 4, and so they were combined into a single category 3.

and Table V 3-15 of Appendix V. While this factor of 3 change would have increased the overall probability of BWR core melt predicted in the draft report by about 20%, the value predicted in the final report has actually decreased by about 30%, as summarized earlier in this section. This clearly illustrates the stability of the overall accident probability predictions made in the study by demonstrating that rather significant changes (factors of 3) in individual contributions have a relatively small effect on the overall result.

COMMENT 5.1.2

It was assumed that the failure of any three adjacent rods to insert results in failure to render the core subcritical. This assumption is described as being conservative and it is questioned why a more realistic determination was not attempted.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

Examination of Table V 3-16 in Appendix V reveals that failure to scram is a significant contributor in the probability of release categories in those specific sequences involving transient events. For transients that occur at full power, as many as four rods in 2 x 2 array must fail to insert before the scram is ineffective because certain peripheral rods have lower reactivity worths than do the rods near the center of the core. However, the major

contributors to scram failure are common mode failures of scram rods and common mode failures due to test and maintenance. These common mode contributions would give essentially the same probability of failure for not only three rods but also for four or more rods. Within the data accuracies, then, the total scram probability of 1.3×10^{-5} applies to either three or four (or more) rod failures.

COMMENT 5.1.3

Since the BWR risks appear to be quite sensitive to the probability of a single rod failing to scram on demand during a transient accident, it is important that the single-rod scram failure probability be accurately assessed. In particular, additional, more extensive data (which are apparently available) should be included in the assessment; the reason for including only two of six reported failures needs to be analyzed and explained; and Acero's[1] analysis should be considered.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

The values for control rod failure used in the draft report were 10^{-4} per demand for an individual control rod failing to insert. Since publication of the draft report, additional BWR control rod failure data were analyzed and again yielded 10^{-4} per demand. Referring to the data in Tables III 4-5 and III 5-3 in Appendix III, it should be noted that Table III 4-5 lists control rod failures of all types. The analysis of interest here is that of a particular failure mode: failure to insert on demand. Of the six BWR control rod failures listed in Table III 4-5, only two were failure to insert on demand.

An estimate based on Acero's approximate rod failure rate of 3×10^{-3} per demand and his values of six demands per year, 145 rods per reactor (average), and 20 reactors would yield approximately 52 rod failures each year. This is not substantiated by operating history even including slow insertion rods. 1973 data show only approximately 10 rod failures of all types. Of these, only two can be considered to satisfy the failure to insert criterion.

COMMENT 5.1.4

Another area that appears to be somewhat questionable in the WASH-1400 analysis of RPS failure occurs in section 5.1 of Appendix II, volume 3. In determining the probability of three adjacent control rods failing to insert on scram demand, consideration is given to common mode failures and a value of 1×10^{-9} was subsequently used to compute the RPS failure probability. The discussion in WASH-1400 seems to imply that the common mode contribution is 0.01 times the single component failure rate. Thus, the actual value to be used, based on this discussion, would appear to be 1×10^{-6}, rather than some combination (in this case, log-normal median) with the uncoupled failure rate. Assuming a value of 1×10^{-6} for three adjacent rods failing to insert, the calculated total BWR risks are raised by a factor of 30 and the average risks correspondingly.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

The study treated the 10^{-6} value as an upper bound for three or more rod failures and treated the independent probability of 10^{-12} as a lower bound. The 10^{-6} value was obtained from the analyses described in Appendix III in which approximately 10% of all failures could be considered as approximating common mode behavior. Since all types of components were considered in obtaining this 10% value and since many of the common modes did not cause failure but only minor degradations, this 10^{-6} value was treated as very conservative and, hence, as being an upper bound.

The coupling treatment discussed in Appendix II, volumes 2 and 3, must also be recognized as being only part of the total dependency analysis that was performed on the RPS. In the actual evaluation, Monte Carlo simulation was performed using the tight coupling and independent values as bounds to obtain

[1] Master's thesis by M. Acero (University of California at Berkely) concluded by fault tree analysis that the probability of a control rod failing to insert on a scram demand is approximately 3×10^{-3}.

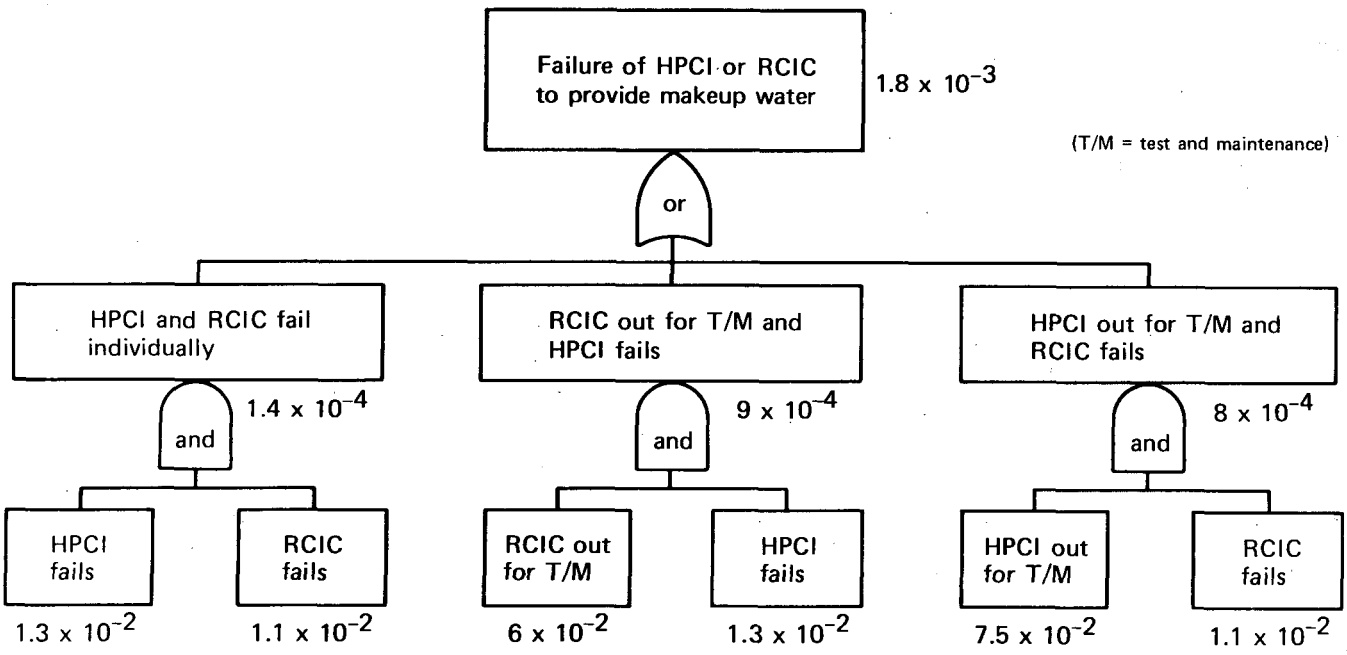


Figure XI 5-1 Corrected Fault Tree for Event U.
(T/M = Test and Maintenance)

the estimated probability distribution and median value for the rod failure dependencies and the RPS total unavailability (as described in section 3.6.2 of Appendix II, volume 1). Furthermore, the failure rate coupling procedure was also used to incorporate dependencies into the rod drop failure rates (as described in section 4 of Appendix IV). The final RPS unavailability was used in event tree quantification and incorporated the Monte Carlo simulation of the tight coupling and independent bounds and the failure rate coupling dependencies as stated in section 4 of Appendix IV.

COMMENT 5.2

For the BWR plant, event U is defined as the availability of the HPCI or RCIC systems for makeup inventory.[1] In determining the failure probability for HPCI and RCIC to provide makeup water, draft WASH-1400 computed the unavailability factors for HPCI and RCIC on the basis they could both be out of service for maintenance at the same time. This situation is not normally allowed by the technical specifications. The correction of this problem should reduce the failure probability of both HPCI and RCIC by about a factor of 6.

(AEC Regulatory Staff)

RESPONSE

The quantification of event U for the BWR transient event tree was indeed conservative for the reason stated in the comment. The analysis below indicates that the likelihood of this event was overestimated by a factor of 4, and section 4.3.2 of Appendix V was modified accordingly. It should be noted, however, that the overall results of the study were not affected because the sequences involving event U were not dominant contributors to the overall release probabilities.

The corrected fault tree from Appendix V is shown in Fig. XI 5-1 (the indicated probabilities are per demand).

This changes the probability of event U by a factor of approximately 4 (i.e., the old value was 8×10^{-3} and the revised value is 2×10^{-3}).

[1] HPCI and RCIC are the acronyms for the BWR high-pressure coolant injection system and the reactor core isolation cooling system. See Appendices I and II for further details of the description and functioning of these systems.

COMMENT 5.3

In Table 2 of Attachment 1 to Appendix V, certain sequences are shown with "containment rupture-vessel steam explosion" failure mode probabilities of zero, which are nevertheless estimated as 0.01 in Table V 3-4 of Appendix V. Since similar tables are not included for the S_1 and S_2 initiating events, the relationship between the various containment failure mode probabilities shown in Tables V 3-5 and V 3-6 of Appendix V cannot be determined (e.g., the relationship between S_2C-δ and S_2C-α).

(U.S. Environmental Protection Agency)

RESPONSE

The containment failure mode probabilities for the large LOCA were used in the draft version of WASH-1400 to assess the small-LOCA (S_1 and S_2) and transient initiated event sequences. Appendix V of this final version of WASH-1400 includes estimates of the containment failure mode probabilities applicable to those dominant core melt sequences for the small-LOCA and transient events.

The S_2C-α sequence was inadvertently omitted from Table V-16 in draft WASH-1400. Table V 3-16 has been corrected (new Table V 3-14), and the relationship between S_2C-α and S_2C-δ can now be seen. The inclusion of S_2C-α provided an important contribution to the category 1 release probabilities for the small-LOCA event; however, it resulted in no significant change in the overall probability results.

5.4 CHECK VALVE RUPTURE

Comments were received on the assessments presented in Appendices I and V for the rupture of the check valve that separates the low-pressure injection system (LPIS) from the PWR reactor coolant system. The specific comments that follow reflect some diversity of views on the LPIS check valve assessments presented in WASH-1400. The reader would find it helpful to refer to Appendix I, section 4.1.6, and Appendix V, section 4.4, where further detail on event V, the check valve accident, is presented.

COMMENT 5.4.1

The probability of the low-pressure injection system check valve failure has been overestimated by one to two orders of magnitude.

(AEC Regulatory Staff; Westinghouse Electric Corp.)

RESPONSE

For the check valve accident, one valve failing open and the second rupturing, the study computes the probability to be about 2×10^{-6} per reactor-year, and Westinghouse computes the probability to be about 2×10^{-8} per reactor-year.

The discrepancy between these calculations arises from two causes. One order of magnitude comes from the difference in rupture probability (1×10^{-8} per hour for the study versus 1×10^{-9} per hour for Westinghouse). The study's data analyses showed that a median value of 10^{-8} was suitable and agreed with available data sources, as indicated in Appendix III. Since Westinghouse has presented no data to support its value of 10^{-9}, the study is unable to discuss the reasons for the differences. (It should be noted that the error spread on the probability estimated by the study is about a factor of 10 and hence covers the Westinghouse value.)

The second part of the discrepancy comes from Westinghouse's use of 10^{-5} per demand for the check valve failing open. The Westinghouse model thus assumes that the check valve failure is independent of time. Since the check valve is never tested for its seating integrity, the study's model treats the check valve as having a time-dependent failure probability of 3×10^{-7} per hour. After 1 year of plant operation, the probability of the valve failing and not being detected is then 3×10^{-7} per hour x 8800 hours per year = 3×10^{-3} (the exact formula is $1 - \exp(-3 \times 10^{-7} \times 8800)$). After 2 years, the probability of failure is approximately 6×10^{-3}; after 3 years, 9×10^{-3}; and so on. The Westinghouse model, on the other hand, always gives 1×10^{-5}, regardless of the amount of time that has elapsed. This difference in treatment accounts for the second order of magnitude difference between the study's result and the Westinghouse result.

One final point about the differences in treatment is worth mentioning. If the valves are tested monthly, then the study's model would give 6×10^{-8}, which is comparable to the Westinghouse result of 2×10^{-8} without testing. The model proposed by Westinghouse would not yield any improvement from testing since the

valve failure probability of 10^{-5} is independent of time and hence independent of testing. The view of the study is that the WASH-1400 model is more realistic and representative of the actual situation.

COMMENT 5.4.2

The piping arrangements may not be typical of PWRs because there is no safety valve on the PWR considered by the study in order to relieve pressure from the high-pressure injection system on the low-pressure injection system piping; thus a dominant PWR accident may be limited to as few as 10 reactors.

(Edison Electric Institute)

RESPONSE

Relief valve provisions did in fact exist in the specific PWR LPIS design considered by the study. These are provided to accept check valve leakage and relieve potential high pressure should the LPIS check valves leak when the interconnecting HPIS is operated. Since event V (a check valve rupture with accompanying dynamic loadings on the LPIS) caused a situation beyond the design intent and capability of the LPIS relief provisions, the simplified schematic in section 4.1.6 of Appendix I did not reflect such provisions and the relief valves were given no credit for system protection in this situation. The design arrangements of valves that lead to the possibility of event V occurring at the PWR studied by the Reactor Safety Study was found to be an important contributor to risk, as indicated by Table V 3-14 of Appendix V. While it is possible that this particular design arrangement is present at only a few PWRs, similar design arrangements, such as the use of in-series motor-operated valves that function as interfacing barriers between high-pressure and low-pressure systems, may exist in other PWR designs. All PWR designs were not covered by the study, however, and, in this sense, the extrapolation of a specific design arrangement to a number of future PWRs where such design arrangements may not apply might be somewhat conservative, as indicated in sections 1.9.7 and 7.4.1 of the Main Report.

COMMENT 5.4.3

There was a possibility that the low-pressure injection system piping might withstand without failure the considerable overpressure produced in the check valve accident sequence; even if it were to fail, there is a chance that the high-pressure injection system and accumulators could provide the cooling necessary to prevent core melting.

(AEC Regulatory Staff)

RESPONSE

The LPIS piping could undoubtedly withstand considerable overpressures if they were gradually applied by check valve leakage. As stated above, the relief valve provisions provided in the LPIS piping design do envision the possibility of gradual leakage. The LPIS design did not anticipate those dynamic loadings that would result from event V, nor did the piping code used for the LPIS piping design require that any particular dynamic analysis be performed. Given the sudden rupture of one of the check valves and the accompanying dynamic loads, it was the judgment of the study that the LPIS failure probability would be near unity. Because the recirculation of coolant to the core depends on the LPIS pumps taking coolant from inside containment and delivering it back to the core, LPIS failure would result in eventual core melt. The emergency core cooling subsystems were extensively discussed in Appendix I, and, as stated in section 4.1.6 of Appendix I, the operation of the HPIS and accumulators could serve to delay core melt but not preclude it.

COMMENT 5.4.4

The discussions in Appendix V seemed to ignore common mode failure of the low-pressure injection system check valves that might be caused by, for example, foreign bodies that entered in the common flow and kept both valves from seating.

(Amory Lovins)

RESPONSE

This comment evidently failed to recognize that event V, in fact, involves a very important common mode failure that had an important impact on the study's results. Section 4.1.6 of Appendix I makes it clear that the general type of potential common mode failure postulated in this comment was considered in the study and all except the LPIS check valve rupture event leading to an uncontrolled LOCA were dismissed for the reasons stated in section 4.1.6 of Appendix I (i.e., "failure of the barriers would

not involve loss of vital safeguards and the loss of normal coolant could be accommodated within the design of the interfacing system through safety and relief provisions, and the coolant loss could be controlled or contained without a core melt occurring"). Should the LPIS check valves experience a more gradual type of leakage from the RCS, as perceived in the comment, the relief valves provided in the LPIS would prevent excessive LPIS loads. Continued operation of the reactor with leakages in excess of 10 gpm is not permitted by terms of the operating license. However, leakages of this magnitude (or somewhat higher by the study's estimate) can be handled by discharge through the LPIS relief provisions without excessive overpressure loadings being encountered. Thus a LOCA due to such leakage would not be expected to occur.

COMMENT 5.5

The derivation of the containment failure pressure utilized in the study and the sensitivity of the overall results to the particular value of the failure pressure have been questioned.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.; Amory Lovins)

RESPONSE

The nominal failure pressure of 100 $\pm$ 15 psia (approximately 1.7 times the design pressure) for the PWR containment structure was derived on the basis of the design criteria utilized and the expected behavior of the structure at loadings in excess of design levels. While considerably above the design pressure, the nominal failure pressure derived is lower than the idealized ultimate strength of the structure in question. The particular containment considered, as well as reactor containments in general, has been strength-tested and leak-tested at internal pressures somewhat above the design level. Satisfactory performance during such testing indicates that the design objectives for the structure have indeed been achieved and lends credence to the expectation that the probability of failure at or near design loadings is very small. As applied in this study, the failure pressure is not represented by a single discrete value, but as a continuous variable with a normal distribution about the nominal value. This approach recognizes that the probability of structural failure is small at loads slightly above design, but increases with increasing loading.

The probability of failure at the nominal failure pressure is taken as 0.5 and approaches unity as the loading approaches the ultimate strength of the structure. The recommendation in the comment above for a minimum failure pressure of 67.5 psia is roughly equivalent to the 2σ lower bound of 70 psia used in the study. In the determination of the containment failure mode probabilities, the potential for containment overpressure failure, in those accident sequences where it is appropriate, has been evaluated for the highest containment pressure expected during the particular accident sequence. Thus the results of the study include consideration of containment failure at less than the nominal failure pressure. Appendix E to Appendix VIII has been rewritten to better clarify the approach taken and the rationale behind the nominal failure pressure selected.

In a number of the accident sequences considered, the containment pressure could potentially rise to levels well above the strength of the containment structure. In such cases, the probability of failure is independent of the value of failure pressure utilized, though the timing of the failure would be determined by the latter. In other sequences, the maximum containment pressure that can be attained is limited because only a limited supply of water is available for contact with the molten fuel and vaporization to steam. Here the potential for overpressure failure does depend on the failure pressure utilized. The assessment of containment failure probabilities for loadings below the nominal failure level takes this possibility into account.

COMMENT 5.6

Describe the methods used to develop the probabilities tabulated in Appendix V from the information presented in Appendix VIII.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

In order to illustrate the methods used to obtain the probabilities of each of the modes of containment failure, the PWR sequence AB, loss of electric power, will be described. The probability of a steam explosion resulting in containment

failure, ABα is $P_\alpha = P_1 = 10^{-2}$, as discussed in section 2.3.2 of Appendix VIII.

The probability of containment isolation failure, ABβ, was determined from fault tree analyses to be $P_2 \simeq 2 \times 10^{-3}$:

$$P_\beta = (1 - P_1)\, P_2$$

$$\simeq 2 \times 10^{-3}.$$

The pressure-time history for this sequence is shown in Fig. VIII 2-7 of Appendix VIII. If hydrogen combustion occurs, the maximum pressure will be 100 psia. The predicted failure pressure is 100 psia, with a standard deviation of 15 psi. Since the maximum pressure is equal to the median failure pressure, the probability of failure is 0.5. As discussed in section 2.3.4 of Appendix VIII, the probability of hydrogen combustion is 0.25. Thus the probability of hydrogen combustion leading to containment failure, ABγ, is $P_3 = 0.125$.

$$P_\gamma = P_3(1 - P_2)(1 - P_1)$$

$$= 0.12.$$

If hydrogen burning does not occur, the peak pressure is 75 psia. This pressure is 1.67 standard deviations below the median failure pressure of 100 psia. The probability of containment overpressurization, ABδ,P_4, can be determined from tables of normal distributions to be 0.048:

$$P_\delta = P_4(1 - P_3)(1 - P_2)(1 - P_1)$$

$$= 0.041.$$

If the other failure modes do not occur, then containment meltthrough, ABε, will be the failure mode:

$$P_\varepsilon = (1 - P_4)(1 - P_3)(1 - P_2)(1 - P_1)$$

$$= 0.82.$$

These probabilities are tabulated in Table V 2-2 of Appendix V.

COMMENT 5.7

With regard to the BWR transients (section 4.3.2 of Appendix I and Table V 3-17 of Appendix V), it is not clear which transients were slow enough so that credit for reserve shutdown can be taken.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

All transients listed under "Likely Initiating Events" in Table I 4-12 of Appendix I can be acceptably handled by the design of the reserve shutdown systems. This is due to the fact that, on a realistic basis, the time rate of effectiveness of liquid poison injection can be considerably slower if termination of power at a rate consistent with preventing fuel melting is considered rather than preventing heat transfer limits (such as those associated with the prevention of the localized departure from nucleate boiling or limiting the reactor coolant system to modest overpressures) from being exceeded. These latter very conservative limits are customarily used in the licensing process. However, exceeding these limits by small amounts does not imply that an accident has occurred or that a radiological consequence to the public will result.

COMMENT 5.8

BWR transient accidents are described and analyzed in section 4.3.2 of Appendix I. The accidents appear to be properly considered except for the assumptions made regarding the likelihood of the initiating event, which seems to be conservative by about a factor of 3.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

The comment indicates that about 10 transient events occur per reactor-year, but points out that only two or three of these transient events would qualify as anticipated transient without scram (ATWS) type events in that they would be more rapid events requiring an immediate core shutdown to prevent core damage. Based on this and ITI interpretations of statements made by the General Electric Co., EPA concludes that a realistic estimate of the frequency of anticipated transients would be about three per reactor-year rather than the value of 10 (with an error band of 2) used in WASH-1400.

The study does not agree that a factor of 3 conservatism is evident in its use of 10 transient events per reactor-year. The comment seems to be concerned with only those more rapid transient events (e.g., MSIV closure, turbine stop valve closures) that could yield the highest predicted fuel enthalpies and RCS pressure levels in the absence of RPS operation (i.e., control rod trip). The study necessarily had to consider all transient events that imposed a demand for RPS operation and for the shutdown cooling systems. As noted by the definitions presented in sections 4.3.1.4 and 4.3.2.4 of Appendix I, it is not proper to limit the study of transient events to those few rapid transients that yielded initial peaks in fuel enthalpy or reactor coolant system pressure. Rather, it is necessary to consider both the initial peaks and the long-term effects that could appear if the core were not to become eventually subcritical or if the core shutdown cooling systems were to fail. Reactor experience clearly indicates that a frequency of about 10 transient events per reactor-year requiring shutdown must be considered.

Section 6

Radioactive Releases from Accident Sequences

Several comments that were received questioned the magnitudes computed for the various radioactive release categories in Appendix V. Each of these comments is discussed in this section.

As a result of these comments and as a part of its preparation of the final report, the study reexamined this area and performed additional computations to better determine the potential radioactive releases for the small-LOCA and transient accident sequences. This effort generally confirmed the study's earlier assessments except for the transient sequences in the BWR that involved potential failures of decay heat removal systems. The reexamination of BWR release category 2 resulted in an increase in the estimated release fractions of the isotopes that are the most significant contributors to potential accident effects. Halogens were increased by a factor of approximately 1.5 and alkali metals by 1.7. These changes and others of lesser significance in BWR release category 2 are shown in Table XI 6-1. Reexamination of the other BWR release categories also led to some adjustment to their values. These changes have been incorporated into section 1 of Appendix V, and into the input to the consequence model described in Appendix VI. A comparison of the significant differences in the magnitudes of the various release categories in the draft and final reports is presented in Table XI 6-1.

COMMENT 6.1

What is the effect of using the consequences of large-LOCA sequences to represent the consequences of transient and small-LOCA accidents?

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

During the preparation of draft WASH-1400, the radioactive releases associated with accident sequences from the large-LOCA event tree were used as a reference basis for establishing releases from sequences associated with the small-LOCA and transient event trees. This was done on the basis of an engineering judgment that the large-LOCA analyses would adequately represent

TABLE XI 6-1 COMPARISON OF THE BWR RELEASE FRACTIONS ESTIMATED IN THE DRAFT AND FINAL REPORTS

Release Category		Fraction of Core Inventory Released											
		I-Br		CS-Rb		Te		Ba-Sr		Ru		La	
Draft	Final	Draft	Final	Draft	Final	Draft	Final	Draft	Final	Draft	Final	Draft	Final
2	2	0.6	0.9	0.3	0.5	0.1	0.3	0.04	0.10	0.07	0.03	2×10^{-3}	4×10^{-3}
3	3	0.08	0.10	0.05	0.1	0.2	0.3	0.03	0.01	0.06	0.02	3×10^{-3}	4×10^{-3}
4[a]		0.10		0.07		0.07		9×10^{-3}		6×10^{-3}		9×10^{-4}	
5	4	0.05	8×10^{-4}	0.02	5×10^{-3}	0.05	4×10^{-3}	2×10^{-3}	6×10^{-4}	3×10^{-3}	6×10^{-4}	-	-
6	5[b]	6×10^{-12}	6×10^{-11}	4×10^{-11}	4×10^{-9}	8×10^{-14}	8×10^{-12}	8×10^{-16}	8×10^{-14}	-	-	-	-

(a) Reexamination of the release magnitudes for the various sequences in categories 3 and 4 indicated that they should merge into one, now termed category 3.

(b) The changes in the release fractions in this category are not of great significance and are due to a reduction in efficiency in assigned radioactivity removal in the standby gas treatment system.

small-LOCA and transient sequences despite some timing differences for the physical processes. After the publication of the draft report, additional calculations were made for the PWR and BWR transient and small-LOCA sequences that dominated the probability of the larger release categories (1 through 4). The results of these additional calculations are incorporated into Appendix V and its Attachment 1. These additional calculations revealed that some changes were needed to more adequately represent the sequences from the other event trees.

Although no changes were necessary in PWR releases, some change did occur in the case of BWR transients involving loss of decay heat removal and containment failure by overpressure prior to core melt. These sequences resulted in the suppression pool temperature being elevated to the saturation temperature, thus leading to a diminished capability of the suppression pool to retain halogens and volatiles piped to the pool through the reactor vessel relief valves. Taken together with the lack of drywell deposition, the overall effect was to increase the magnitude of radioactive releases to the atmosphere. The most significant change, in BWR release category 2, involved increases in the potential releases of halogens and alkali metals by 50 and 70%, respectively. The potential releases of alkaline earths and tellurium also increased in factors of 2.5 and 3, respectively. These changes were incorporated into the final report.

COMMENT 6.2

The strontium releases used for core meltdown accidents appear to be too low because (1) data from some experiments with small specimens show that maximum releases of more than 50% could occur; (2) they are based on gradual, rather than uniform, core melting; and (3) they are less than the 50% value used in WASH-740.

(Richard E. Webb)

RESPONSE

The first point apparently refers to data discussed in Appendix D to Appendix VII of draft WASH-1400. It is true that some individual experiments have produced strontium releases of more than 50%. However, many factors must be considered in interpreting such results. Releases vary with external atmosphere, type and size of specimen, type of heating, duration of high temperature, and gas flow conditions. In addition, scatter in experimental data is commonly found in experimental work of this type. The experimental data must be examined in toto rather than by considering only isolated points, and the experimental conditions should be correlated with the expected accident conditions. On this basis, the high strontium release values obtained in some experiments are of questionable applicability and should be given a low weight in evaluating the trend of the body of the data.

Regarding the second point, complete core meltdown is assumed in WASH-1400 in specifying the strontium as well as other isotopic releases. An important factor in determining the amount of radioactivity released from the fuel as it melts (as well as at later times), is its surface-to-volume ratio. Thus, if the fuel pellets were to drop into a pool of molten fuel before melting, the releases would be much smaller than those resulting from pellets melting individually before dropping. As the WASH-1400 calculations of radioactive releases are based on data from experiments on small samples, this is the equivalent of assuming that melting occurs on an almost pellet-by-pellet basis. Actually, since it is expected that much of the release of radioactivity would be governed by situations in which a much smaller surface-to-volume ratio is expected, the predicted releases are likely conservative, as pointed out in section 7.4.1 of the Main Report.

With regard to the third point, it was estimated in Appendix VII that strontium releases for core meltdown accidents could range from 2.2 up to 25%.[1] The best-estimate value used to perform realistic consequence calculations was 11%. Comparison against the WASH-740 value is not valid because the latter was not based on applicable data or on the type of analyses performed in Appendix VII.[2]

---

[1] These values include the contribution from the vaporization release component.

[2] WASH-740 (p. 23) identifies the strontium release value used as a "conservative guess" for meltdown and combustion of metallic fuel.

COMMENT 6.3

The decontamination factor of 1000 used in CORRAL-PWR calculations (Appendix V in the section entitled "Results of CORRAL-PWR Calculations") for soil leakage of radioactive materials other than noble gases and organic iodine should be justified.

(American Physical Society
Study Group on
Reactor Safety;
Amory Lovins)

RESPONSE

A justification for the selection of this particular soil decontamination factor is given in section 3.3.3 of Appendix VII. In addition to the thoughts presented in Appendix VII, it is noted that the extent of radionuclide trapping by the soil would probably vary among reactor sites due to differences in subsurface soil conditions. Calculations show that, even if the soil decontamination factor varied by as much as an order of magnitude (either up or down), the calculated total release of radioactivity to the atmosphere would change by less than a factor of 2. In other words, the amount of radioactivity that could potentially escape through the ground after containment meltthrough is smaller than the amount that would escape from above-ground leakage from containment to the atmosphere prior to meltthrough even if the soil decontamination factor were as low as 100.

COMMENT 6.4

It would be useful to examine the sensitivity of CORRAL results to the degree of mixing of compartment contents, in order to establish the conservatism of the "well-mixed" assumption.

(Atomic Industrial Forum)

RESPONSE

The "well-mixed" assumption used in CORRAL is considered to be more realistic than conservative in terms of defining the actual conditions that could occur during a core meltdown accident. In fact, because of the physical phenomena occurring, it is more difficult to believe that significant mixing will not occur rather than that it will. In cases where the containment sprays operate, experimental work[1] has showed that mixing within and between compartments is enhanced. In accident sequences where containment sprays do not operate, the presence of the concentrated heat source in the core and the generation of appreciable quantities of gases also promote circulation. One also has to consider that the "well-mixed" assumption has both positive and negative effects on accident consequence predictions (i.e., it is not clearly conservative or nonconservative). For example, if poorer mixing occurred, concentrations would vary between compartments. Since the total removal factor for certain mechanisms is concentration dependent, variations in the total amount of radioactivity available for release would result. Such potential effects are covered by the smoothing technique described in section 3.1.2.1 of this appendix and section 4.1.2 of Appendix V.

COMMENT 6.5

In Table 5.1 of the Main Report, it was noted that it was not evident how the differences in noble gas releases of 100% for the BWR and 20-90% for the PWR are derived.

(General Electric Co.)

RESPONSE

As noted, BWR release categories 1 through 3 have 100% of the noble gases released from containment, whereas PWR release categories 1 through 5 involve somewhat smaller releases. As indicated in Tables 4 and 11 of Attachment 1 to Appendix V, core melt in both PWRs and BWRs leads to the release of essentially 100% of the noble gases from the fuel to the containment. However, since the containment volume is significantly larger in the PWR, the puff release of containment atmosphere, given containment failure, would result in the release of only a portion of the containment atmosphere before a quasi-equilibrium is established. The magnitude of this puff is governed by the conditions within containment (pressure and temperature) at the time of containment failure. Leakage thereafter is

[1] R. C. Schmitt, G. E. Bingham, and J. A. Norberg, Simulated Design Basis Accident Tests of the Carolinas-Virginia Tube Reactor Containment - Final Report, IN-1403, Idaho Nuclear Corp., December 1970.

relatively low and is associated with the generation of gases by decay heat.

COMMENT 6.6

The core inventory release fractions employed in RSS were understated by as much as a factor of 2.... Among the considerations involved were problems regarding the conversion of technetium and ruthenium from the molten core to possible volatile oxides by bubble-through of carbon dioxide from concrete decomposition. RSS acknowledges uncertainties in Appendix VII in the question of expected volatilization of dozens of radioactive compounds.

(Union of Concerned Scientists)

RESPONSE

This comment addresses the release of radioactivity from the core to the containment atmosphere in potential accident sequences in which the core has melted through the bottom of the reactor vessel and is interacting with the concrete floor of the containment building. As discussed in Appendix VII, release from the fuel consists of four major components: gap release; meltdown release; vaporization release caused by internal convection and sparging by the gaseous products of concrete decomposition; and, where appropriate, oxidation release following a steam explosion. The accident sequences under discussion here do not involve potential steam explosions.

Table VII 2-1 of Appendix VII indicates that the sum of the gap, meltdown, and vaporization release components is 8% of the core inventory for the noble metal group (Ru, Mo, Pd, Rh, and Tc). This sum is composed principally of a meltdown release of 3% and a vaporization release fraction of 5%. As is also indicated in Appendix VII, some uncertainty exists about the amount of noble metals that could be released since, if they were to combine with oxygen, they could be released in larger quantities than would be the case if oxygen were not present. The noble metals are expected to exist in metallic form mixed into the iron phase of the molten systems and as such would be released in relatively small amounts (<1%). Although sparging by carbon dioxide[1] would create an oxidizing environment within the melt, the noble metals are not expected to oxidize substantially since the oxygen will combine preferentially with the iron in the mix. To account for the possibility of some localized oxidation of the noble metals by carbon dioxide sparging, a 5% vaporization release was used, rather than the value of less than 1% that would be appropriate if no allowance for oxidation were made. Thus a factor of 5 has already been included in the estimated value of noble metal release to account for potential uncertainties due to their oxidation.

[1]The carbon dioxide would be created by the decomposition of the limestone in the concrete floor by the interaction with the molten fuel.

Section 7

Emergency Cooling Functionability

Comments pertaining to emergency cooling functionability (ECF) for the large-LOCA event tree were received from three sources.[1] The principal concern expressed was with the basis for the choice of its failure probability, with the comments ranging from criticism of the study for using a failure rate too low to criticism for using a value too high. Some also suggested that the emergency core cooling system (ECCS) had no chance of success and that the study should have employed a failure probability of 1.

The question of the success or failure of ECCS -- as a matter of functionability, as opposed to operability -- does not readily lend itself to analysis by the methods used in WASH-1400. Thus, the study decided to examine what level of failure probability would cause ECF to contribute to potential accident risks. As noted in Appendix V, section 4.2, sensitivity studies reveal that "... even if values as high as 10^{-1} for ECF failure (probability) were to be used, any contribution made would be within the accuracy of the overall calculations."

Thus, although there appears to be no current basis for making a rigorous quantitative assessment of the probability of ECF failure, the analysis referenced showed that even if ECF failure probability were as high as 10^{-1}, it would not change the results of the study significantly. It is the view of the study that the probability that ECCS will fail to cool the core adequately is less than 10^{-1}.

---

[1] U.S. Environmental Protection Agency; Westinghouse Electric Corp.; Amory Lovins.

Section 8

Reactor Vessel Rupture

COMMENTS

Five sources[1] made comments on this subject ranging from statements that the probability value used for reactor vessel rupture ($10^{-7\pm1}$ per vessel-year) was too high to statements that it was too low. Some comments also stated that contradictory evidence was ignored.

RESPONSE

The following sections of draft WASH-1400 discussed the possibility and treatment of potential reactor vessel rupture in considerable detail:

a. Main Report, sections 5.3.2.4 and 5.3.4.2

b. Appendix I, sections 4.1.4 and 4.2.4

c. Appendix V, section 4.5

A review of these sections and the comments received indicates no reason for changing the substance of the sections as written in the draft report. However, these discussions would have been more complete if section 4.5 of Appendix V had noted the publication of the U.S. Atomic Energy Commission Regulatory Staff Report, WASH-1318, Technical Report on Analysis of Pressure Vessel Statistics from Fossil-Fueled Power Plant Service and Assessment of Reactor Vessel Reliability in Nuclear Power Plant Service, in May 1974. The principal conclusions of that report, based on the analysis of 725,000 vessel-years of service in U.S. fossil-fueled power plants, are generally consistent with the analyses performed by the study and the Advisory Committee on Reactor Safeguards (ACRS). The principal conclusions of WASH-1318 are that the upper limit (99% confidence) probability of a disruptive failure event in any one nuclear reactor vessel during any service year falls within the range of 10^{-7} to 10^{-6}, and the actual value of this probability would be expected to be even smaller.

More comprehensive studies by the USNRC Staff, which are currently under way, indicate that the failure probability may potentially be reduced by an additional factor of 10 or 100. This conclusion is based on a detailed investigation of the influence and scheduling of the periodic inspections that reactor vessels are expected to receive during their service lifetime.

Concern about the adequacy of reactor pressure vessels has been expressed by such distinguished people as Sir Alan Cottrell and F. R. Farmer of the United Kingdom and Monroe Wechsler of the United States. The study and the ACRS considered all available failure rate data, including the extensive body of data developed by British and German sources. Although there is some opinion in the United Kingdom that the probability of catastrophic failure of the reactor pressure vessel should be about 10^{-5} per reactor-year, the study does not believe that this value is very realistic. As noted in section 5.3.2.4 of the Main Report, even if the probability of vessel rupture were as high as 10^{-5} per reactor-year, it would then just begin to contribute appreciably to the overall risk and would not change the results of the study.

For the convenience of the reader, the pertinent sections of WASH-1400 referenced earlier are summarized here. Sections 4.1.4 and 4.2.4 of Appendix I, which consider the various kinds of vessel ruptures that could occur in PWRs and BWRs, respectively, categorized ruptures according to size and location. Certain of these breaks are equivalent to pipe breaks, and emergency core cooling systems would be able to cool the core successfully. Since the probability of vessel breaks is far smaller than that of pipe ruptures and the consequences of accidents that might proceed in this general way would be no larger than those associated with pipe breaks, these types of breaks would not represent a significant contribution to overall risk. Potentially large ruptures in the vessel, a subgroup of all

[1] AEC Regulatory Staff; Atomic Industrial Forum; Union of Concerned Scientists; Amory Lovins; Richard E. Webb.

possible vessel ruptures, could prevent effective cooling of the core by the emergency core cooling systems. Depending on the details of the event, as described in the study, core melt vessel failures could occur in an intact or nonintact containment and, for the BWR, in an oxidizing or nonoxidizing environment.[1]

Thus, these types of vessel failures can cause a fairly broad range of consequences. Nevertheless, the contribution to overall risk was shown to be essentially negligible when the probabilities of such failures were taken into account.

As indicated in section 4.5 of Appendix V, the principal basis for assigning numerical values to the probability of large ruptures in pressure vessels was the statistical analysis of the extensive failure data base by the ACRS.[2] The ACRS reached the following conclusion:

"There is reasonable assurance that: (1) the disruptive failure probability of non-nuclear vessels in central station service by modes pertinent to reactor vessels is less than 1×10^{-5} per vessel-year, (2) the disruptive failure probability of reactor vessels designed, constructed, and operated to Sections III and XI of the Code is less than 1×10^{-6} per vessel-year, and, (3) the disruptive failure probability of such reactor vessels, beyond the capability of engineered safety features is even lower."

The study's analysis and review of British and German pressure vessel failure data generally agreed with these results, and a value of 10^{-7} was used as the median estimate of failure probability for reactor-vessel ruptures large enough to be beyond the capability of emergency core cooling systems. A probability range of a factor of 10 was associated with this value, which gave an upper bound of 10^{-6}, coinciding with the ACRS value for any such ruptures.

In summary, the study has presented evidence from recent published reports based on extensive reviews of all published data to support the use of the value of 10^{-7} per vessel-year for the failure probability of reactor pressure vessels. The study has also considered the opinion of authorities who appear to hold different views, but it has seen no other firm data to support the selection of a different value for reactor vessel failure probability. To reemphasize a point made earlier, it is estimated that the failure probability would have to be 100 times larger than estimated in order to begin to be an appreciable contributor to the predicted risk.

---

[1] BWR containment buildings are generally filled with an inert (nitrogen) atmosphere. Depending on the particular accident sequence involved, fuel melting can occur in the inert atmosphere or, if the containment fails in a certain way, in an air (oxidizing) atmosphere. The oxidizing properties of the containment atmosphere can thus affect the selective release magnitudes of various radioactive isotopes, such as ruthenium.

[2] Advisory Committee on Reactor Safeguards, Integrity of Reactor Vessels for Light Water Cooled Reactors, January 1974.

Section 9

Large Nuclear Excursions

COMMENT

Comments received from two sources pertained to potentially large nuclear excursions. The subjects addressed were the lack of detailed discussion of the phenomenology of very fast transients (excursions); the desire for further information supporting the evaluation of the probabilities assigned to "worst-case" transients (i.e., the BWR control rod ejection and the PWR cold-water accidents); and the completeness of the arguments with respect to the magnitude of consequences associated with such accidents and thus to their overall contribution to risk.

(AEC Regulatory Staff; Richard E. Webb)

RESPONSE

It is apparent that the import of the discussion contained in Appendix I, section 4.3, apparently did not communicate adequately to those who made the above comments. The discussion that follows is an attempt to clarify that section of Appendix I.

In particular, Figs. I 4-12 and I 4-13 for the PWR and BWR, respectively, classify transient events by frequency of occurrence and then provide a rough (but correct) differentiation of the probability of core melt due to the various potential transient events. These results show very clearly that the likelihood of core melt events is dominated by anticipated transients and that lower likelihood events, such as the potential rod ejection accident in BWRs and the cold-water accident in PWRs, do not contribute significantly to this probability. This is indicated in Tables I 4-9 and I 4-12 in Appendix I. Nevertheless, to clarify the matter even further, analyses of both these potential accidents, including their probability of occurrence and their potential consequences, are presented below.

BWR ROD EJECTION ACCIDENT

A failure of one of the control rod drive housings that are welded to the bottom of the pressure vessel is a prerequisite to having the potential for control rod ejection. This postulated

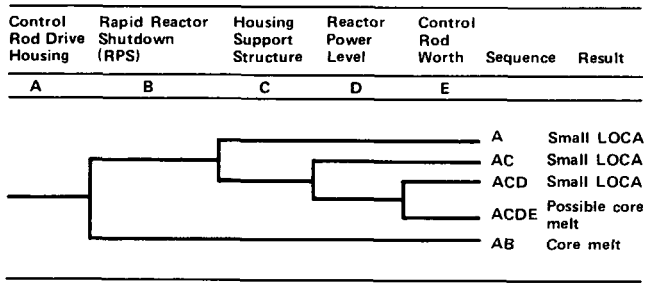


Figure XI 9-1. Event Tree

failure, under almost all conditions, results in a small LOCA and is analyzed by the small-LOCA (S_2) event tree (see Appendix I, section 4.2.2). In order for the failure of a control rod drive housing to lead to fuel damage, a control rod with a reactivity worth greater than 1.5% $\Delta k/k$ must be ejected from the core. This requires that (1) the reactor be critical but at less than 20% power, (2) the control rod drive housing support structure fail (allowing the control rod to eject), and (3) the ejected control rod be one of the rods having a reactivity worth large enough to cause localized melting.

A simplified event tree, in which ACDE is the sequence of interest for the BWR rod ejection accident, is shown in Fig. XI 9-1.

For the events in Fig. XI 9-1 the following failure probabilities have been generally conservatively estimated:

Event	Failure Probability
A - Control rod drive housing	$\sim 10^{-4}$ per reactor-year
B - Rapid reactor shutdown (RPS)	$\sim 4 \times 10^{-6}$ to 5×10^{-4} per demand
C - Housing support structure	$\sim 10^{-3}$ to 10^{-2}
D - Reactor power level	$\sim 2 \times 10^{-3}$ to 2×10^{-2}
E - Control rod worth	<0.1

The above failure probabilities were determined as follows:

Event A. Control Rod Drive Housing

The control rod drive housing forms part of the pressure vessel and has the same manufacturing and inspection requirements as the balance of the pressure vessel. As discussed in section 4.5 of Appendix V, the pressure vessel disruptive failure probability is less than 10^{-6} per reactor-year.

Another method to establish the failure rate of the control rod drive housings would be to analyze these housings as dead-ended pipe stubs extending from the bottom of the pressure vessel. The median probability of all LOCA-interfacing ruptures in this size range (2 to 6 inches) is estimated to be approximately 3×10^{-4} per reactor-year (see section 6.4 of Appendix III). The total "dead-ended piping" making up the control rod drive housing is less than one-third of the total LOCA-sensitive piping. Therefore, the probability of the housing failure would be approximately $1/3 \times 3 \times 10^{-4}$, or about 10^{-4} per reactor-year.

Using the pipe failure data as a conservative estimate, the probability of a control rod driving failure can be assigned a value of 10^{-4} per reactor-year.

Event B. Rapid Reactor Shutdown (RPS)

The failure probability is determined by fault tree analysis in Appendix II, volume III, section 6.2.

Event C. Housing Support Structure

The failure of the housing support structure could be a structural failure when loaded or a failure of not being reinstalled after being removed for maintenance on the control rod drive system. Since the support structure is designed with large structural safety margins, it is considered highly unlikely that it would fail and allow rod ejection to occur. However, the structure is periodically removed for reactor maintenance purposes; it is thus possible for a portion of the structure not to be replaced properly after maintenance. The failure probability of the structure would thus be dominated by the maintenance contribution. From the human performance data presented in section 6.1 of Appendix III, this failure is estimated to be approximately 10^{-3} to 10^{-2} per event.

Event D. Reactor Power Level 20%

There are approximately 13 events per year that involve operation of the reactor in the range from critical to 20% power. Assuming a median value of 4 hours in this power range per event, it is estimated that the plant will be in this power range approximately 52 hours per year. Therefore, the probability of being in this lower power range (P_C) is approximately 52 hr/8760 hr $\simeq 6 \times 10^{-3}$ per event.

Event E. High Worth Rods

During startup, when approximately 50% of the control rods have been withdrawn from the core, analysis indicates that approximately 10% of the inserted rods have a reactivity worth equal to or greater than 1.5% $\Delta k/k$.[1] This represents the maximum number of high-worth rods that could be present at any time during startup. As power level is increased to 20%, only those control rods adjacent to the last in-sequence rod withdrawn from the core have the potential for reactivity worths in excess of 1.5% $\Delta k/k$. Thus, only four of the total of 185 rods can be involved at any one time during the ascent to 20% power.

For this analysis it is conservatively assumed that 10% of the rods are high-worth rods for the power range of concern (i.e., from critical to 20% of normal full power). Therefore, the probability (P_D) of the ejected rod being a high-worth rod is assumed to be approximately 10^{-1}.

Using the upper bounds of the values indicated above, it is found that accident sequence ACDE yields a value of approximately 2×10^{-9} per reactor-year.[2] Even if these postulated core melt events are quantified by using conservatively high failure rates, their probability is negligibly small compared

---

[1] When 50% of the control rods have been withdrawn, the core is still subcritical or has just attained criticality at zero power.

[2] The potential for dependencies between these events has been examined. The design of the housing support structure is such that it is unlikely that failure of a control rod housing would cause it to fail.

to that of other transient events identified in the Reactor Safety Study.

In regard to the potential consequences of such an event, the reactivity transient resulting from the rod ejection accident postulated above will lead to the rapid melting of about a 2-foot section of the four fuel assemblies adjacent to the ejected rod (0.09% of the core). The energy generated in the transient is relatively small (much less than the core decay energy integrated over 1 minute). Thus, the transient would not significantly affect the radioactivity inventory of the core. While it is conceivable that the molten fuel might be dispersed and rapidly transmit its stored energy to the coolant, it is considered highly unlikely that such dispersal of relatively small amounts of fuel into the coolant would cause damage to the reactor vessel or the reactor coolant system. Some distortion of fuel assemblies might occur, however, which potentially could interfere with the ability of the engineered safety features to adequately cool the core after the transient. Even if one were to consider such a situation as an upper bound, a rod ejection accident could clearly do no more than rupture the coolant system and the containment in a manner similar to the steam explosion (α) containment failure mode. This could lead to radioactivity releases similar to those in BWR release category 1. However, because of its low probability (approximately three orders of magnitude lower than that of BWR release category 1), the rod ejection accident would not contribute to the overall risk.

PWR COLD-WATER ADDITION ACCIDENTS

As indicated in Fig. I 4-11, Table I 4-9, and the associated discussions in section 4.3 of Appendix I, cold-water addition accidents were considered in the development of the PWR transient event tree. As indicated on Fig. I 4-10, this type of transient is classified under general unanticipated transients; that is, transients whose frequency of occurrence would be expected to be about 10^{-5} per reactor-year. The following discussion develops this description in greater detail.

The PWR analyzed is equipped with main reactor coolant system loop isolation valves. With these valves closed, an isolated loop will cool down well below the normal operating temperature. If the valves were then to be opened with the pump in this loop running, a quantity of cold water could be added to the core, causing a reactivity transient because of the increased density of the cold water relative to reactor coolant at operating temperature. To prevent inadvertent operation of these valves during power operation, administrative procedures require that the unit be brought to zero load and the temperature of the isolated loop be brought to within 10 F of the temperature of the active loops prior to opening the loop isolation valves. Furthermore, the reactor protection grade interlocks that are provided prevent the isolation valves from being opened unless (1) the temperature in the isolated loop is within 20 F of the corresponding temperature in the other loops and (2) a minimum flow of at least 400 gpm has been maintained in the closed loop via a bypass line for at least 1 hour to permit the temperature in the closed loop to be raised to that of the operating loops by pump heating. Thus, a cold-water addition accident at the plant analyzed requires multiple failures of independent interlocks (having a failure rate of about $10^{-3\pm1}$) plus an operating error by the reactor operator. Because such an error would have to involve a direct violation of operating procedures, it is reasonable to assign this a value of $10^{-3\pm1}$. Thus the probability that both the interlock will fail and the operator will make the error is $(10^{-3\pm1})^2$. The estimated upper and lower bounds on the probability of both failures occurring at the same time are 3×10^{-5} and 4×10^{-8}, respectively, with a log-normal median value[1] of 10^{-6}.

---

[1]The log-normal median and error bounds are determined as follows:

$$P = 10^{-3\pm1} \times 10^{-3\pm1} = 10^{-(6\pm\sqrt{1^2+1^2})}$$

$$= 10^{-6\pm1.4}.$$

Thus, the median value is 10^{-6}, the upper bound is $10^{-4.6} \simeq 3 \times 10^{-5}$, and the lower bound is $10^{-7.4} \simeq 4 \times 10^{-8}$.

Analyses have been performed to determine the consequences of a cold-water addition accident. They indicate that, at the worst time in the fuel cycle (end-of-life conditions) and with the core at zero power, the peak reactor power reached would be approximately 65% of rated power. The addition of cold water under these conditions would produce the greatest reactivity insertion rate. The core is not expected to experience a departure from nucleate boiling, and no fuel damage or radioactivity release is anticipated.

Thus, a cold-water addition accident has a small probability of occurrence and would not lead to fuel damage even if it occurred at the worst time in the core life. Therefore, the PWR cold-water addition accident was determined to be a negligible contributor to risk.

Section 10

Behavior of Radionuclides in Soil and Water

COMMENT 10.1

Comments were received regarding the analysis of the potential for contamination of water bodies by the migration of radioactivity through the soil under the influence of groundwater.

(U.S. Department of the Interior
Nuclear Energy Liability
Property Insurance Association)

RESPONSE

The analyses presented in draft Appendix VII have been modified to include consideration of groundwater contamination by the release of spray water to the soil-water system, release of airborne activity to the groundwater system during containment vessel depressurization after containment vessel meltthrough, and groundwater leaching of the core mass after containment meltthrough (see section 3.3.4 of Appendix VII). It was found that the first two cases could be combined into a single depressurization release case. Examination of the results presented in Appendix VII indicates that for the depressurization case, the concentrations of ruthenium-106, strontium-90, and cesium-137 in the groundwater will be above the maximum permissible concentrations (MPC) given in 10CFR20 at the time the groundwater enters the water body. For the leaching case, only strontium-90 will be above MPC.

As also noted in Appendix VII, it should be emphasized that the hydraulic model parameters, the radionuclide distribution coefficients, and the radionuclide leaching rate used in the analyses were selected to produce overestimates of the rate of appearance of the radionuclide sources at the groundwater outlet to the water body. For example, since the soil permeability coefficient used in the calculations is indicative of well-sorted sands with gravel and of fissured limestone formations, the distribution coefficients are probably low by factors of 10 or 100. The leaching expression assumes a relatively highly soluble glass containing fissures that increase the effective surface area by a factor of 100 or more. In addition, calculations of the human radiation dose resulting from use of the receiving water body would have to include the dilution effect that would occur in the water body beyond the efflux point for the contaminated groundwater. At the time of the peak discharge rate, the strontium-90 in the efflux would exceed the maximum permissible concentration by a factor of about 23. If, for example, the receiving water body is a relatively small river with a flow rate of 13,000 cfs, the peak strontium-90 concentration in the river for the depressurization release case will be 100,000 times lower than that in the groundwater and will be well below the maximum permissible concentration. Potential peak concentrations of this type would not occur until approximately 6 years after the meltthrough accident, and mitigating actions could be taken to prevent the migration of radionuclides to the water resource, as discussed below. Similarly, if the receiving water body is a large lake with a volume of 15×10^6 acre-feet and uniform mixing is assumed, the concentration of strontium-90 in the lake will be approximately 50% of the maximum permissible concentration for strontium-90 in water, assuming no removal processes in the lake and no flushing of the lake by additional fresh water. Thus, at many sites the groundwater contamination problem is expected to be very much less severe than indicated in Appendix VII.

Another important factor to consider in evaluating the above results is the time required for the movement of radionuclides through a groundwater system. Several months and in many cases years should elapse before contamination would appear in water bodies used for the support of a significant population group. This delay would allow ample time for instituting monitoring operations and for setting up an effective warning network. More importantly, the time would most likely be used to execute procedures for controlling or even eliminating the spread of contamination beyond the reactor site. This would involve drilling wells for monitoring and pumping purposes to control the local groundwater flow gradient. The withdrawn water could be stored temporarily in surface tanks or in sealed holding ponds for subsequent

treatment. After the movement of the radionuclides is under control, it would seem feasible, if it were considered necessary, to form a vaultlike barrier around the radioactive zone using a combination of excavation, drilling, and concrete injection operations.

Even without the above engineered mitigating actions, the basic conclusion of the analysis would not be changed. Specifically, the analysis has shown that hydrologic contamination occurs on a much longer time scale than does atmospheric contamination for a core melt-through accident. Therefore, warning actions alone should be sufficient to limit population radiation doses from hydrologic sources to low levels in comparison with the doses received from atmospheric sources.

COMMENT 10.2

The porosity of the ground was omitted in the computation of the volumetric rate of fluid delivery for the hydraulics model. Proper inclusion would raise calculated groundwater effluent concentrations by a factor of 5.

(U.S. Department of the Interior)

RESPONSE

The volumetric rate of fluid delivery was calculated from the equation

$$F = kAG,$$

where

F = volumetric flow rate (ft^3/day)

k = soil permeability coefficient (ft^3/day-ft^2 at unit gradient)

A = cross-sectional area of soil channel (ft^2)

G = groundwater slope or gradient (ft/ft).

The standard definition of k takes into account soil porosity. The permeability coefficient times the gradient must thus be multiplied by the actual soil cross section, not the pore cross section. Therefore, the calculated volumetric flow rate and the effluent concentrations are correct as given in Appendix VII.

COMMENT 10.3

Equation VII 3-10 in Appendix VII is not applicable because it pertains to a solid soil region, which in reality would be a cylindrical hole left by the molten core.

(U.S. Department of the Interior)

RESPONSE

The equation in question is entirely valid because it specifically applies to the period of initial containment melt-through and for perhaps a few hours beyond. Analyses do not support the contention that during this period the melt will create a cavity in the underlying soil.

Section 11

Core Melt Analysis

COMMENT 11.1

It has been suggested that the consequences of partial core melting could be more severe than those of complete melting. Specifically, a reviewer suggests that "the greater surface area, for example, could cause more extensive steam explosions."

(The National Intervenors)

RESPONSE

It is expected that, all other things being equal, the consequences of partial core melting will be less severe than those associated with complete melting. Although the total surface area of the separate fuel rods in their initial array is greater than that of a large molten mass, it is smaller than the surface areas attainable on the dispersion of the molten mass into small particles. In order to contribute to steam explosions, fuel or structural materials must be in the molten or vaporized state; heat cannot be transferred sufficiently rapidly from bulk materials to water to contribute to damaging steam explosions. Thus, for a given molten particle size distribution, the energy transferred in a steam explosion will vary directly with the amount of material melted. The analysis discussed in Appendix VIII is based on the assumption the 80% of the core mass is dispersed as small particles.

COMMENT 11.2

The applicability to both PWRs and BWRs of a single set of results illustrating the effect of decay time on the core meltdown sequences discussed in Appendix VIII has been questioned.

(General Electric Co.)

RESPONSE

The specific power differences between a PWR and a BWR would lead to differences in adiabatic core heatup rates. However, the results illustrated in the particular figure in question include the effects of metal-water reactions and the boiloff of water in the core. The quantities of cladding as well as water in the core are different for the two types of reactors. Taking into account these effects, together with uncertainties in the analyses, it was found that a single set of curves could indeed represent the results for both PWRs and BWRs.

COMMENT 11.3

The question has been raised "as to whether vessel failure can occur by fracture due to thermal stress occurring when the molten core contacts the lower vessel head."

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

Conceptually extremely high thermal stresses can be produced on contact between the vessel head and the molten core. Such high thermal stresses would be localized near the surface and would be accommodated by plastic flow of the material affected. At the temperature levels of interest here (i.e., at or above normal operating levels) the pressure vessel materials would exhibit ductile behavior, and fracture as a result of localized thermal stresses would not be expected.

COMMENT 11.4

It appears that the radioactive source term is based on 3200 MW(t) in all cases, but a power level of 2441 MW(t) is assumed for PWR meltdown calculations. This anomaly should be resolved.

(The Detroit Edison Co.)

RESPONSE

Radioactive source term calculations are based on an assumed power level of 3200 MW(t) for both PWRs and BWRs. However, as noted in chapter 1, section 19, of the Main Report, two plants were used as the basis for the study. The PWR plant considered, the largest PWR about to start commercial operation with developed operating procedures, has a maximum thermal power level of 2441 MW. Since the meltdown calculations performed in Appendix VIII require details of core

geometry, the PWR plant under study was analyzed. It should be noted, however, that the absolute power level of the core is not the controlling factor in core meltdown. Rather, power density is important. The peak and average linear heat generation rates and power densities are comparable for cores operating at the two power levels, and hence the choice of a 2441-MW(t) core for thermal analyses will not introduce any significant error. Thus, basing the timing of meltdown processes on a thermal analysis for a power level of 2441 MW(t) is not inconsistent with the use of a radioactive inventory based on 3200 MW(t).

Section 12
Steam Explosions

COMMENT 12.1

A number of questions and comments were received regarding the analysis of steam explosions. Specific points that have been raised include (1) the potential for steam explosions at times other than those considered in the study (e.g., delayed entry of PWR accumulator water during small LOCAs and transients); (2) the significance of water subcooling; (3) the lack of experimental verification of the analytical models; and (4) the conservatism of the predicted results.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.; Amory Lovins)

RESPONSE

As acknowledged in WASH-1400, the evaluation of the potential for, and consequences of, steam explosions that may be associated with reactor meltdown accidents involves considerable uncertainty. There are no directly applicable experimental data that can be used to guide the analyses. On the one hand, no violent interactions have been observed in small-scale experiments with uranium dioxide and water. On the other hand, there have been a substantial number of industrial incidents in which contact between molten materials and water has led to explosive interactions; a number of these incidents are summarized in Appendix B to Appendix VIII. In the face of limited experimental data, the quantitative evaluation of the probability of steam explosions and their potential effects has required considerable use of engineering judgment. Several of the points that have been questioned are discussed below.

It is recognized that the potential for interaction between molten core materials and water exists during much of the course of a meltdown accident. At two key points in the accident sequence (i.e., at the time the molten core falls to the bottom of the reactor vessel and at the time of reactor vessel meltthrough) there is the possibility that large quantities of molten material will rapidly come into contact with water. These are the instances in which the potential for damaging steam explosions is believed to be the greatest and are the cases explicitly considered in the study's analyses. As noted in sections 2.2.1.3 and 2.2.1.4 of Appendix I and in sections 2.2.7 and 2.2.8 of Appendix VIII, steam explosions that might occur in the PWR reactor vessel cavity region after reactor vessel meltthrough were considered but were determined to have no important impact on the containment rupture probabilities. This conclusion would hold regardless of whether or not the steam explosion occurred as a result of molten materials dropping into residual water in the cavity or by a delayed discharge of accumulator water on the molten mass in the cavity region. When water is introduced at the top of the melt or when the molten core comes into contact with moist soil or groundwater, the potential for the coherent interaction of a large quantity of molten material with water is much smaller since the water cannot readily penetrate into or displace the high-temperature melt. If a significant interaction were to occur on containment meltthrough, the effect on overall consequences would be small since such an interaction would have no additional effect on containment integrity.

A number of experimental programs (cited in Appendix B to Appendix VIII) on the interaction of molten materials (particularly metals) with water, have shown that the potential for violent interaction decreases as the subcooling of the water decreases. This observation has been taken into account in the study's analyses by assigning a higher probability for the occurrence of explosive interactions in the presence of subcooled water than in the presence of steam-saturated water. Furthermore, the occurrence of steam explosions with steam-saturated water has not been precluded. The damage potential was taken to be independent of the temperature of the water.

COMMENT 12.2

The dismissal of the potential for a large energy release from a steam explosion occurring when the molten core comes into contact with the water-laden gravel beneath the containment floor

seems to be contradicted by the Armco incident described in Appendix VIII.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

The analyses discussed in Appendix C to Appendix VIII indicated that a large fraction of the stored energy of the molten core had to be transferred rapidly to the generation of steam in order to develop the mechanical energy required to threaten containment. Such a transfer of energy requires the coherent interaction of a significant quantity of hot molten material with water. These conditions were at least partially met in the Armco incident, where a large quantity of molten steel was dropped from a height of 40 feet onto damp ground. This apparently resulted in a series of small "explosions," and not a coherent interaction. In the event of a core melt accident, the contact between the molten core and the moisture in the gravel would not be rapid, as is indicated in section 2.2.6 of Appendix VIII, and thus a coherent large-scale interaction would not be expected.

Section 13
Hydrogen Combustion

COMMENT 13.1

The available experimental data on flammability and detonation limits in air-hydrogen-steam mixtures are limited and accordingly the conclusions regarding the potential of containment failure due to these mechanisms are questioned.

(Amory Lovins)

RESPONSE

The scarcity of directly applicable data on flammability and detonation limits on air-hydrogen-steam mixtures was recognized and acknowledged by the study (see Appendix D to Appendix VIII). The containment failure mode probabilities that have been derived are based on both the probability of the occurrence of these phenomena and their effects should these phenomena take place. The probabilities of hydrogen burning or detonation were based on the limited data available together with consideration of the containment conditions that would exist during each accident sequence; these are subject to considerable uncertainty. As noted in Appendix D to Appendix VIII, the flammability limits used probably represent the minimum compositions for flame propagation. Furthermore, since the results of the study are not sensitive to detonation-limit predictions, the uncertainties associated with the flammability and detonation limits used in the study do not have a particularly significant effect. The effects on containment integrity of hydrogen burning or detonation, should either occur, are more readily calculable; these effects will vary with the different accident sequences.

COMMENT 13.2

The conclusion in section 2.2.1 of Appendix I that noncondensable gases cannot overpressurize PWR containment seems inconsistent with BMI-1910.[1]

(Amory Lovins)

RESPONSE

There is no inconsistency between BMI-1910 and WASH-1400 in regard to the effects of noncondensable gases on containment failure. BMI-1910 presented upper limits for the possible effect of noncondensable gases while clearly stating (page 25) that "it should not be presumed from Figure 12 that reactions to this extent are possible within the containment." Moreover, the upper limit results in BMI-1910 are compared with the design pressure of the containment. Since the analysis in WASH-1400 is performed on a realistic basis, the pressure at which the containment would be expected to fail is of interest and the design pressure is not. Clearly, there is a substantial difference between the design pressure and the failure pressure of a reactor containment building.

For the case considered in WASH-1400, the partial pressure of the hydrogen (due to the complete reaction of the Zircaloy cladding, the lower core support structure, and the reactor vessel bottom head) is about 18 psi. The contribution from the carbon dioxide generated by concrete decomposition is about 12 psi; that of the air initially present in the containment is 9 psi. Thus, at the time of containment melt-through, the maximum partial pressure of noncondensable gases would be about 39 psi. Since the containment design pressure is 45 psig (60 psia), it seems that this pressure should not cause it to fail.

COMMENT 13.3

The assumption of uniform mixing of the hydrogen with the containment atmosphere is questioned.

(Amory Lovins)

RESPONSE

In order to present a threat to containment integrity by rapid burning, hydrogen must react with the oxygen in

---

[1] D. L. Morrison et al., An Evaluation of the Applicability of Existing Data to the Analytical Description of a Nuclear Reactor Accident - Core Meltdown Evaluation, BMI-1910, Battelle Memorial Institute.

the containment. The complete reaction of the hydrogen generated would require a substantial fraction of the available oxygen in the containment and thus would require good dispersal of the hydrogen to yield high-energy releases. Unless the hydrogen is dispersed throughout the containment, such a complete reaction would not be possible. Partial reaction of the available hydrogen either by burning or explosion, as might be expected for nonuniform hydrogen distributions, would result in lower containment pressures than those associated with uniform mixing.

COMMENT 13.4

Comments have been received regarding the possibility of hydrogen generation by the interaction of molten structural materials with water and the possible impact on the potential for containment failure of the burning or detonation of this hydrogen.

(Louis Baker; Amory Lovins)

RESPONSE

The PWR core meltdown analyses presented in Appendix VIII indicated that the equivalent of 75 ± 25% of the Zircaloy cladding could be expected to react with water during the initial core meltdown process if sufficient water were available. The potential for containment failure due to hydrogen burning or detonation, as presented in Attachment 1 to Appendix V, was evaluated on the basis of hydrogen generation from the reaction of 75% of the cladding unless the reaction was limited by water availability.

The reaction with water of the core lower support structures and the reactor vessel bottom head after reactor vessel meltthrough would produce about five times the hydrogen generated by the complete reaction of the Zircaloy cladding.

Although large quantities of hydrogen can conceivably be generated from the reaction of molten structural materials with water, the extent of hydrogen burning within the containment would be limited by the quantity of contained oxygen. In the PWR containment considered in the study, there is enough oxygen to react with the quantity of hydrogen that would be generated by a 150% reaction of the cladding. If such a quantity of hydrogen were to react with oxygen by detonation or deflagration, the containment pressure would exceed its expected failure level. This rapid consumption of all the oxygen within containment presupposes the dispersal of hydrogen throughout all parts of the containment. If the extent of reaction is less than that represented by the complete consumption of the available oxygen, the maximum possible pressure in the containment will not be attained and the probability of containment failure will be lower.

In considering the possible effect of added hydrogen generation on containment failure probabilities, it is convenient to divide the accident sequences under consideration into three categories:

a. Sequences in which containment failure precedes core melting.

b. Sequences involving core melt in combination with failure of the containment recirculation sprays or containment heat removal systems, followed by containment failure.

c. Sequences in which the containment recirculation sprays and removal systems operate throughout the course of the accident.

Each of these categories will be discussed in turn.

a. Containment Failure Precedes Core Melting

The generation of additional hydrogen has little effect on these sequences. Core melting and hydrogen generation take place in a failed containment. The burning of hydrogen in a failed containment could temporarily increase the driving force for release, but this would exert very little effect on the consequences.

b. Meltdown Precedes Containment Failure in Combination with Failure of Containment Recirculation Sprays or Containment Heat Removal Systems

Core meltdown combined with the failure of the containment recirculation sprays generally leads to a high probability of containment failure due to overpressure. Where appropriate, the effect of the burning of hydrogen generated during initial core melting has been included in the evaluation of these sequences and has been found to produce a noticeable contribution to the probability, but a small effect on the timing of containment failure. The additional hydrogen from the steel-water reaction could conceivably further increase the potential for containment failure. However, except for cases where the

availability of water to the pressure vessel is limited, the probability of containment failure due to overpressure is already quite high (0.4 to 1.0), and the effect of additional hydrogen generation would not increase the probability of overpressure failure by more than a factor of about 2. Furthermore, the generation rate of this additional hydrogen is uncertain, and in some cases significant quantities of hydrogen may not be available until after containment failure.

There are also a few sequences in this category in which the potential for containment overpressure failure as presented in Attachment 1 to Appendix V is limited by the availability of water to the melt. If in these sequences the available water reacts with steel to generate hydrogen and the latter burns, the potential for containment failure could be increased. Because the containment atmosphere is at elevated temperature and pressure in these sequences, however, the potential for the ignition of the hydrogen-air-steam mixture would be decreased and the occurrence of complete combustion would be unlikely. Thus, it is expected that these effects should counter balance and, within the accuracy of such calculations, no important change in either the probability or release magnitude is anticipated for these sequences.

In the PWR core melt sequences in which the containment heat removal system fails but the recirculation sprays are operating, containment overpressure failure and containment meltthrough are predicted to take place at about the same time. In these sequences, the burning of the additional hydrogen could reduce the time at which overpressure failure might occur. Here again, however, the containment atmosphere at the times of interest would be at elevated temperature and pressure, thus reducing the potential for the occurrence of self-propagating hydrogen combustion.

c. Meltdown with Sprays and Containment Heat Removal Operating

In the third category of accident sequences, the containment recirculation sprays and heat removal systems operate throughout the meltdown event and containment pressures are kept at low levels. Under these assumptions, there is no possibility of containment overpressurization, as analyzed in Attachment 1 to Appendix V, and containment meltthrough is the most likely failure mode. If hydrogen were to burn as it is generated, the released energy would be absorbed by the sprays and would have no effect on the failure modes analyzed. However, when the additional hydrogen from the steel-water reaction is considered and a delayed detonation or deflagration is assumed to occur when a stoichiometric hydrogen-air mixture is attained, containment failure is indicated. The probability of such a reaction, requiring the consumption of all the oxygen within the containment and the rapid propagation of the flame front to all parts of the containment volume, is difficult to assess. Since this reaction would require a quantity of hydrogen equivalent to that generated by the reaction of 150% of the cladding and the dispersal of this hydrogen throughout the containment, it could only take place at some time after core meltdown (i.e., sufficient time would have to be available for a significant steel-water reaction).
For a significant reaction with water, the steel must be at or near its melting temperature. A large mass of molten steel (together with the fuel and cladding) would present only a limited surface area for reaction with water (steam). The reaction rate could be further limited by the accumulation of oxides at the molten surface and by the evolution of hydrogen, both tending to prevent the access of water to unreacted metal. Thus, while a substantial reaction between molten structural material and water is possible, it would probably require an appreciable period of time.

Most of the radioactivity release from the fuel takes place during the initial core melting. With the containment sprays operating, there would be relatively little activity in the containment atmosphere at the time of containment failure due to hydrogen detonation. Thus, while the maximum possible detonation or deflagration of the hydrogen could lead to a containment failure mode not previously considered for these sequences, the potential consequences of this failure mode would not differ greatly from those previously evaluated.

The core release fractions[1] associated with overpressure failure due to the detonation or deflagration of the additional hydrogen, assuming containment

[1]Release fractions represent integral release fractions at the time of containment vessel failure.

failure 4.5 hours after a large LOCA with ECR failure (1 hour after reactor vessel meltthrough), are estimated to be as follows:

Noble gases: 0.86
Organic halides: 0.003
Halogens: 0.0026
Alkali metals: 0.009
Tellurium: 0.029
Alkaline earths: 8.7×10^{-4}
Noble metals: 0.0018
Lanthanides and actinides: 3.4×10^{-4}

Examination of Table V 2-1 of Appendix V indicates that, for the isotopes that dominate the consequence calculations (see Appendix VI), these releases compare well with those associated with PWR release category 5.

As noted above, the rate of hydrogen generation by the steel-water reaction is difficult to assess with confidence. Equally difficult to assess is the probability that hydrogen will burn not on generation but only on reaching a stoichimetric mixture with oxygen.

Detailed analyses have not been performed to assess the probability of occurrence of the releases associated with delayed hydrogen generation and subsequent detonation or deflagration; however, it is likely that their probability of occurrence is only a small fraction of the probability of occurrence of the particular PWR release category.

Section 14

Data Base

COMMENT 14.1

Nine sources submitted comments on the study's evaluation of human actions.[1] These ranged from assertions that the human failure rates estimated in Table III 6-4 of Appendix III were too high to assertions that it is not possible to predict human errors.

RESPONSE

The assignment of failure rates to human actions, though somewhat more subjective than the assignment of failure rates to hardware, is not without a measured data base from which to start. The general human error rate estimates presented in Table III 6-4 of Appendix III were derived from actual experience in nonnuclear activities as assessed by the study's human reliability analysts. It should be recognized that Table III 6-4 presents general, illustrative values. For application to a specific situation, these must be modified by consideration of the inputs available to an operator (displays on control panels, audible alarms, labels, equipment configuration, the presence and quality of written procedures, etc.), the stress level to which an operator is exposed, and the required operator response and feedback available after the response. In addition, personnel redundancy must also be considered. For example, approximately 30 minutes after the occurrence of a large LOCA with the emergency core cooling system operable, two valves in parallel are opened to establish flow from the containment sump to the suction of the low-head safety injection pump. The basic error rate associated with this act, as given in Table III 6-4 of Appendix III, is 10^{-1}. Considering the presence of at least three operators in the control room at that time, the probability that all operators will independently neglect to open the valves at the time specified is estimated to be 10^{-3}. Furthermore, the availability of visual indication of refueling water storage tank level in the control room can reduce the probability of failing to open the valves to 10^{-4} per action.

Similarly, Table III 6-4 suggests that the probability of misselecting the valve switches and operating the wrong valves is 10^{-1}. However, considering the layout of the control board, the extensive training given to operators in this area, and the fact that the operation of valves most likely to be mistakenly operated is required in the next step of the procedures, the probability of human error in this specific instance has been assessed to be 10^{-2}.

As noted in Appendix III, the assessment of human errors is somewhat subjective, and data obtained from several nonnuclear activities have been used. Human factor rates were assessed as realistically as possible considering the available information. Probability ranges were incorporated to account for variations in the assessment of human error rates and in the extrapolation of data to nuclear applications. Within the accuracy required for risk calculations, the study believes the human data, with its range, to be sufficient. The study also believes, however, that more effort in the future devoted to a better understanding and modeling of human reliability factors would be useful.

COMMENT 14.2

Comments received from two sources were directed to the possibility that operator action might mitigate the probability or consequences of an accident.

(Edison Electric Institute; Sargent & Lundy Engineers)

RESPONSE

Operator action to mitigate accident probabilities or consequences was considered as a viable option when written procedures suggesting that such actions be taken were available or when an extended period of time was available for an operator to analyze the situation or obtain offsite assistance. Credit for operator action was not given when it appeared that such actions would have

---

[1] U.S. Environmental Protection Agency; Electric Power Research Institute; Atomic Industrial Forum; Babcock & Wilcox; Bechtel Power Corp.; Westinghouse Electric Corp.; Friends of the Earth; The National Intervenors; Union of Concerned Scientists; Amory Lovins.

to be taken in a short time period and there was no evidence that the operator had procedures or prior training instructing that such actions be taken.

COMMENT 14.3

Comments received from four sources suggested that the human failure analysis was invalid because quality assurance errors were not included.

(U.S. Environmental Protection Agency;
Nuclear Energy Liability Property Insurance Association;
Iowa Student Public Interest Research Group;
The National Intervenors)

RESPONSE

As indicated in section 3.1.4 of this appendix, the data base used to determine equipment failure rates included failures attributable to design, manufacture, installation, and maintenance errors that were not detected by quality assurance programs. Thus, quality assurance errors are implicitly included in the study's equipment failure data base and the associated error spreads.

COMMENT 14.4

There is a question as to whether the data base used in the study is representative of what can be expected from reactor plant components.

(Federal Energy Agency)

RESPONSE

The study attempted to make the best assessments of failure data on the basis of currently available information. As stated in Appendix III, error spreads were used to show the uncertainties and variabilities associated with the estimated failure rates. The failure rates determined from the data base are compared with existing data from nuclear power plants in Table III 4-2 of Appendix III. As indicated therein, the available nuclear data fall within the assessed range of equipment failure rates. However, the study believes, as indicated in section 7.4.2 of the Main Report, that data should be collected and analyzed for nuclear plants to permit more precise predictions of component and system behavior.

COMMENT 14.5

The statistical basis (FPC instability data) for choosing 10^{-3} as the probability of offsite power loss at the time of a LOCA seems weak, in that the loss of offsite power is more likely to be caused by malfunctions other than instability.

(AEC Regulatory Staff)

RESPONSE

It should be noted that the failure of offsite power in conjunction with a LOCA is of interest only in the relatively short period of time after a LOCA occurs. While it is true that there are causes for the failure of offsite power other than instability, they are quite unlikely to occur in the LOCA time window. However, there will surely be a transient on the electrical grid supply to the site at the time of a LOCA. Thus, instability data are the most suitable basis for failure probability calculations.

COMMENT 14.6

Anomalies in Table III 4-1, for example, that Liquid Metal Engineering Center failure rate data fall 3x outside the assumed range for motors, 200 to 2000x for pipes should be fully explained.

(Amory Lovins)

RESPONSE

As explained in Appendix III, the ranges assigned to the data are not deterministic bounds and therefore do not necessarily include all the source data. Thus, all source data need not fall within the assigned ranges. (It should be noted that in the calculations, the log-normal distributions themselves were used, and not the ranges.) Also, as explained in Appendix III, the ranges and distributions were not derived from simple empirical fits but involved some subjective judgments and decisions. Sensitivity studies were performed to investigate possible additional variations in the components mentioned, and few significant effects were obtained.

COMMENT 14.7

In section 4.2.2.2 of the Main Report it is stated that even with large component failure rate uncertainties, the system failure probabilities were sufficiently accurate to yield meaningful values for risk evaluation. It would be helpful in establishing the credibility of using

large uncertainty limits if proof of this were developed further. For example, in Table 5.4 of the Main Report, an upper bound for core melt probability is 2×10^{-4} per reactor-year. This appears to be unrealistically high.

(Bechtel Power Corp.)

RESPONSE

The error spreads on the component failure rate were propagated by standard statistical techniques to obtain the error spreads on the system and accident sequence probabilities. As seen in the report, these system and accident sequence error spreads were generally one order of magnitude (or less) in size. Because order-of-magnitude results were acceptable for risk assessment, the size of the system and accident sequence error spreads formed the basis for the statement that system failure probabilities were sufficiently accurate for the purposes of the study. Based on present data, the study does not feel that the bounds for core melt are conservative.

COMMENT 14.8

In our opinion, the probability of failure (severance) of large nuclear pipe should be reduced by an order of magnitude, which yields an estimated occurrence rate of about 10^{-5} per reactor-year. The probability of severance of a small pipe in nuclear service should also be lower, although perhaps not by a full order of magnitude.

As a further example of the conservatism that appears to have been used in the selection of failure rates for LOCA-initiating events, it was assumed that 5% of all piping in a plant, or about 8500 feet of piping, is large-LOCA sensitive; that is, it could lead to a large LOCA, if ruptured. This assumption is very conservative.

(AEC Regulatory Staff)

RESPONSE

The assessment of pipe failure data is discussed in detail in section 6.4 of appendix III. Reported failures are generally derived on a per plant basis. Therefore, to obtain a LOCA-sensitive piping failure rate, the failures per plant-year from data must be multiplied by the ratio of LOCA-sensitive piping to the total piping for which piping failures are reported rather than to the total installed piping in the plant. Appendix III has been clarified in this regard.

COMMENT 14.9

Comments were received from four sources relative to the treatment of the effect of aging on the failure rates. The thrust of these comments is that the effects of plant and component aging, or at least the variation of failure rates with time, should be explicitly recognized and taken into account.

(Nuclear Energy Liability Property Insurance Association; Scientists Institute for Public Information; The National Intervenors; Amory Lovins)

RESPONSE

As stated in the report, the study's calculations (as described in Appendix II, volume 1) apply to steady-state behavior and were not intended to include significant aging effects or life-cycle trends. Aging is a separate question that perhaps could be analyzed when and if data are available and, more importantly, if the need to do so clearly existed. The study has also stated that its results should not be extrapolated beyond the first 100 plants expected to be operating in the next 5 years and has suggested that a future study like WASH-1400 be repeated in about 5 years.

COMMENT 14.10

Several comments that were received questioned the study's handling of component data and its treatment of random variables and confidence intervals. A formal Bayesian treatment was suggested as being a better approach.

(Engineering Decision Analysis Co.; General Electric Co.; Edison Electric Institute; Union of Concerned Scientists; Amory Lovins)

RESPONSE

The draft version of WASH-1400 was not as precise as it could have been in discussing the probabilistic approach used in the study's quantifications. Appendix II, volume 1, and Appendix III, in particular, have been rewritten to better clarify the rationale and method-

ology that served as the basis for the study's probabilistic approach.[1]

The failure rates, and component data in general, were treated as being random variables based on the variability observed in the data sources and on the intended application of the calculated probabilities to a population of 100 plants. The failure rates were not constrained to be in any given finite interval and a log-normal distribution was selected as adequately describing the variability observed in the failure rates cited by the various data sources examined.

This observed variability was taken as being representative of the variability that would exist in the population of 100 plants. (As described in Appendix II, volume 1, this representation was not inconsistent with available nuclear data.[2]) The calculations, however, must be interpreted as being conditional on the employed data distributions.

The confidence bounds used in the study are probability ranges, with associated percentiles, which served to summarize the probability distribution of the system characteristics (e.g., system unavailabilities). Because of the random-variable data treatment, the system characteristics were treated as being not formal probabilities but estimators (random variables). The simulation approach, using 1200 trials, was of sufficient precision for the order-of-magnitude results calculated. A formal Bayesian approach was not used, because raw failure data (e.g., times of failure) were not employed, but instead reported failure rates were used as input information. As described in Appendix II, volume 1, however, the study's results can be interpreted in a general Bayesian framework, where the data distributions are interpreted as the given priors.

---

[1] For further information on the use of the random-variable approach, see for example, N. R. Mann, R. E. Schafer, and N. D. Singpurwalla, Methods for Statistical Analyses of Reliability and Life Data, John Wiley and Sons, Inc., New York, 1974.

[2] Because of the broadly scattered nature of the data, including the nuclear data, the formal hypothesis tests performed were somewhat questionable.

Section 15

External Forces

COMMENT 15.1

The effects of near-site explosions as a potential cause of reactor accidents are not considered.

(U.S. Environmental Protection Agency)

RESPONSE

Near-site explosions were considered but not explicitly analyzed in the study because a significant potential for large explosions does not exist at most reactor sites. This is discussed in section 2.1.3.1 of this appendix and in Addendum I to the Main Report.

Those reactors that are located in the vicinity of industrial installations having the potential for explosive accidents or shipping routes routinely involving the transport of large quantities of hazardous material are subjected to detailed investigation in this regard during the licensing process of the particular reactor to determine the potential effect of an explosion on the nuclear power generating facility. Such reactors are provided with additional protection, if required, to reduce the probability of a significant accident that might potentially result from an offsite explosion to a negligible value. As a final point it should be noted that even if an explosion were to occur near the site of a reactor not so protected, the massive structures provided for tornado and seismic protection and for radiation shielding give nuclear facilities a considerable degree of explosion protection.

COMMENT 15.2

Floods that exceed the Probable Maximum Flood should be considered. Further, the effect of floods on structures other than the containment should be considered. In addition, the severe effects of the flood on communications may make a large evacuation unrealistic.

(U.S. Department of the Interior)

RESPONSE

The probability of a flood equal to or greater than a Probable Maximum Flood (PMF) is discussed in section 5.4.3 of the Main Report. As indicated therein, analyses suggest that the probability of such floods is low. Analyses performed to date are somewhat limited, however, and it is recognized that there may be a somewhat higher possibility of large floods in rivers other than that analyzed. It is suggested that analyses be performed in the future to develop a more valid statistical model for the overall effects of floods in risk assessment.

All critical features of the plant that are required for safety are protected to the PMF level. Thus, structures other than the containment that house such equipment are protected.

Evacuation after a severe flood might indeed be difficult. However, if a flood larger than the PMF were to occur, most people originally located in the flood plain would probably have been evacuated before the flood. Those evacuated to higher elevations would be centrally located in evacuation centers and easily contacted if further evacuation were warranted in the event of a flood-induced reactor accident. It should be recognized that the warning time associated with a large flood would generally permit the marshalling of large civil defense and military efforts to assist in flood evacuation which would be available in the event of a flood-induced reactor accident.

COMMENT 15.3

A number of comments were received indicating seismic effects were inadequately considered. These comments stated that the estimate of the probability of large earthquakes is in error, that the logic used to determine the likelihood of multiple-system failures after an earthquake is not obvious, that a number of sites with differing geologic structures and seismic activities should have been considered, and that the AEC regulatory

staff method of estimating earthquake risks is questionable.

(AEC Regulatory Staff;
U.S. Department of the Interior;
General Electric Co.,
Bechtel Power Corp.,
Division of Reactor Research & Development;
Engineering Decision Analysis Co.,
Union of Concerned Scientists)

In regard to the probability of large earthquakes, it should be noted that the analysis in the draft report predicted the probability of an earthquake that would exceed the safe shutdown earthquake (SSE) (about 0.2 g) generally used for reactors east of the Rocky Mountains. The value predicted, $10^{-5\pm1}$, was derived from analyses that were based on data presented by Algermissen[1] and Cornell and Mertz,[2], who predicted the probability of occurrence of various-size earthquakes in 100,000 square kilometer areas and attenuation factors for earthquake size as a function of distance from the epicenter of the quake.

The final report takes advantage of more recently published information,[3] which integrates the work of a number of people to predict the probability of earthquakes of various sizes occurring at any point in the eastern United States. This work, as described in section 5.4.1 of the Main Report, predicts the probability of a 0.2-g earthquake to be 20 to 50 times higher than the median value used in draft WASH-1400. While these predicted values are probably somewhat conservative, the final report has been modified to use them.

The logic used for predicting the probability of failure of systems given the occurrence of an SSE was based on the results of a check of the implementation of seismic design requirements, as described in section 2.1 of this appendix and in Appendix X. Since about 10% of those items checked were thought to have some deficiencies in seismic design, a system failure probability of 10^{-1} given the SSE, was assigned to each safety system.

A recent report by Newmark[4] indicates that large safety factors are incorporated into the seismic design of reactor safety systems. These safety factors would make the probability of failure of a system about 0.15% in a reactor subjected to an SSE. Furthermore, the report indicates that substantial margin to failure exists for earthquakes that are significantly larger than the SSE. The combination of these factors with the earthquake frequency predictions by Hseih discussed earlier led to an overall predicted probability of core melt of about 10^{-8} and 10^{-6} per reactor-year for all sizes of earthquakes. This would not contribute significantly to the probability of core melt of 5×10^{-5} predicted from all other causes predicted by the study.

In regard to the consideration of sites of different geologic structures and seismic activities, it should be noted that the work of Hseih, since it is a prediction of earthquake probability for any point in the eastern United States, covers sites of different geologic structures. This same work also covers a wide range of seismic magnitudes. As already indicated, the analysis in the final report incorporates this information and indicates that the predictions of earthquake damage are also generally valid for west coast sites.

---

[1] S. T. Algermissen, "Seismic Risk Studies of the United States," Proc. 4th World Conference of Earthquake Eng., Santiago, Chile, 1969.

[2] C. A. Cornell and H. Mertz, "A Seismic Risk Analysis of Boston," paper presented at the National Conference of the American Society of Civil Engineers, April 1974.

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

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

One comment questioned the validity of the approach used by the regulatory staff in the selection of design basis earthquakes. While the study did not use this method, it is noted that the analysis in section 5.4.1 of the Main Report assumes that reactor sites are randomly located relative to earthquake epicenters. It should be recognized that this is a conservative approach since the regulatory process tries to ensure that reactors are not located in the near vicinity of potentially active earthquake faults. Assuming that reactors are located randomly with respect to earthquake epicenters gives no credit for the application of regulatory siting requirements. The study believes that the regulatory method is valid and, in fact, results in earthquake risks for reactors being smaller than that assumed in the study's approach.

Section 16
Sabotage

Several comments[1] noted the need to evaluate the susceptibility of nuclear power plants to acts of sabotage and to evaluate the possible consequences thereof. This subject had been considered by the study in the draft report, and it was concluded that the probability of occurrence of such acts could not be estimated, but that the consequences of such acts would not be greater than the largest consequences estimated from other causes. It was also stated to be difficult for an act of sabotage to create consequences as large as the largest predicted from other causes.

Further examination of this area has since been completed. The overall view of the study concerning sabotage is presented below. The discussions of sabotage in the Main Report (sections 1.9(3), 5.4.6, and 7.4.2) have also been modified as appropriate.

The results of the investigation of sabotage have led the study to the following conclusions:

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

2. Recommendations for further countermeasures have been made. Some of these have already been acted on, 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 U.S. NRC guidelines (Safety Guide 1.17 and proposed Section 73.55 10CFR), 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.

---

[1] American Physical Society Study Group on Reactor Safety; Pollution and Environmental Problems, Inc.; Resources for the Future, Inc.; The National Intervenors; Union of Concerned Scientists; R. Keller; Amory Lovins; Richard E. Webb.

Section 17

Scope

Comments were received from eight sources[1] relative to certain aspects of the scope of the study. These comments generally suggested that the study would be improved if it were modified to include high temperature gas-cooled reactors (HTGRs), liquid metal fast breeder reactors (LMFBRs), fuel reprocessing plants, transportation accidents, and the use of mixed oxide fuel.

As noted in section 1.1 of the Main Report, the "principal purpose of the 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." section 1.9 of the Main Report states this study covers only light-water cooled nuclear power plants of the type now coming into operation. Other types of nuclear facilities were outside the scope of this analysis. Furthermore, the type of analysis performed in WASH-1400 requires the final designs of plants and detailed operating, test, maintenance, and emergency procedures. Such information is not available for facilities other than light-water reactors, and therefore a WASH-1400 type of analysis could not have been performed even if it were desired to do so. It is true that less detailed, more generalized risk assessments can be performed for such facilities; however, the analyses would be less rigorous.

Comments were also made to the effect that the study should recognize the design differences between the plants analyzed and other light-water reactors and present the necessary arguments to support the thesis that differences at the system level do not have a major effect on overall risk assessment.

Furthermore, the validity of extrapolating results to 100 reactors should be discussed, particularly with respect to the plant mix expected to be in existence in the future.

The objective established at the outset of the study was to look ahead only to the near future -- that is, the reactor plant mix expected to be in operation in about 5 years. Thus, the upper limits of extrapolation appeared to be a population of 100 plants consisting of approximately equal numbers of PWRs and BWRs.

The two plants analyzed were selected on the basis that they were the largest plant of each type about to start operation.[2] As indicated in section 1.9 of the Main Report, the applicable codes and standards and safety design requirements have been significantly improved since the designs of the plants considered in the study were undertaken. Chapter 7 of the Main Report discusses in some detail the validity of the extrapolation to 100 reactors and suggests that such extrapolation is likely to be conservative for the above reasons as well as improved implementation of design requirements. Chapter 7 also suggests that "it would be useful to pursue these matters further to give a greater degree of confidence in the extrapolation of results to other plants."

---

[1] U.S. Department of Health, Education and Welfare; U.S. Environmental Protection Agency; Atomic Industrial Forum; Babcock & Wilcox; Pollution and Environmental Problems, Inc. Resources for the Future, Inc.; Sargent & Lundy Engineers; Union of Concerned Scientists.

[2] It was necessary to choose plants very near the commencement of operation to ensure the availability of final designs plus operating, test, maintenance, and emergency procedures needed for detailed analysis.

Section 18

Design Adequacy

Several comments that were received suggested clarification of various sections of Appendix X or were editorial in nature. Where appropriate, changes have been made in the text of Appendix X to clarify the intent and remove ambiguities. A number of specific comments required a response in kind, often accompanied by a textual change in Appendix X. These are presented below.

COMMENT 18.1

For the PWR reactor building, a constant damping of 10% of critical damping was employed for the design basis earthquake, as noted in section A6.3.1.1. Although it is not possible, because of the limited data available, to confirm that this assumption is sufficiently conservative, we note that damping associated with the first mode shown in Table X A-13, if predominantly rocking, appears larger than we have normally used for rigid-body rocking motion.

(Gibbs & Hill, Inc.)

RESPONSE

The damping coefficient used for the rocking mode is 10% of the critical damping coefficient and is obtained from the ratio of the strain released to the energy stored in the structure when responding to this particular mode. This method of estimating the modal damping coefficient, coupled with the classical analysis of structural response with foundation interaction, has been proved by Roesset et al.[1] to provide reasonably accurate results.

COMMENT 18.2

In section A6.3.1.1, the report states that the effective mass of the soil, estimated to be approximately 25% of the mass of the base mat or less than 10% of the mass of the building, was not considered in the analysis but was of "minor consequence." No effective mass moment of inertia of soil has been mentioned which may influence the response.

Moreover, our experience indicates that in vertical translation the effective mass of the soil is much larger than for the horizontal translation and should not generally be neglected in the analysis since its effects may significantly alter the response.

(Gibbs & Hill, Inc.)

RESPONSE

The role played by soil mass and soil inertia in the structural response is not uncontroversial. However, the omission of these effects in the model is not regarded as contrary to good engineering, state-of-the-art, practice. Some investigators[2] believe that these parameters play a minor role.

COMMENT 18.3

In section A6.3.2.3 of WASH-1400, Appendix X, it is stated that for both nozzles, Bijlaard's method of analysis is of doubtful value for the computation of the stresses in the pump casing wall at the junction with the nozzle, since the conditions for valid application of Bijlaard's method are not present.

The comments on the limitations of Bijlaard's method are theoretically correct, however, as in most real engineering problems some approximations must be made to arrive at a solution.

Use of the Bijlaard method with appropriate approximations which make the method feasible, shows that the design

---

[1] J. M. Roesset, R. V. Whitman, and R. Dobry, "Modal Analysis for Structures with Foundation Interaction," Journal of the Structural Division, Proceedings of the American Society of Civil Engineers, March 1974, p. 399-416.

[2] R. V. Whitman and F. E. Richart, Jr., "Design Procedures for Dynamically Loaded Foundations," Journal of the Soil Mechanics and Foundations Division, Proceedings of the American Society of Civil Engineers, November 1967.

is adequate for its intended use. The results for one load case comparison show that the maximum stress occurs at the same location and differs by only 1%. Further, finite element evaluations will be made which more closely approximate the true geometry, loadings and boundary conditions. These additional analyses are considered as only back-up to existing analyses and are not required to establish design adequacy.

(Westinghouse Electric Corp.)

RESPONSE

The information that was presented for consideration was not a detailed stress analysis of the actual discharge nozzle and casing. Rather, two geometrically simpler (and therefore more tractable) problems were examined:

a. The intersection of a small cylinder (analogous to the nozzle) and a larger uniform cylinder (analogous to the pump casing).

b. A similar cylindrical/spherical shell intersection problem.

The actual stress was then estimated from these results by comparing the solved geometries with the actual geometry.

This approach can provide acceptable evidence of structural adequacy in either of the following cases:

a. The comparison stresses from the simplified models are within allowable stress levels, and it can be clearly demonstrated that the comparison stresses conservatively bound the actual solution.

b. The comparison stresses are much lower than the permitted limits, so that actual stresses will be acceptable even if the comparison stresses are unconservative estimates.

In the case of the discharge nozzle, the calculated comparison stresses are quite large. Under upset conditions, reported stress intensities for casing surfaces are essentially at the limit (slightly below if typical as-built thicknesses are used; and slightly above if minimum casing thicknesses specified in the drawings are used). For the faulted condition, local membrane stress intensity is shown to be 67% to 79% of the limit (depending on the thickness assumption made).

Comparison Model	Stress (psi)
Cylindrical vessel:	
NUMBRA program	63,671
Bijlaard's Table 5	64,216
Calculated with initial load stresses	54,378
Spherical vessel:(a)	
SPHNOZ program	61,530
Bijlaard's Table 2	61,536 (solid nozzle)
Bijlaard's Table 3	57,325 (hollow nozzle)

(a) The spherical vessel model is taken to have a radius equal to the diameter of the cylindrical model. This is the "mean" radius of curvature of the cylinder.

Before the stress values from the comparison models can be accepted as valid for geometries that depart from those modeled, it must be determined whether the stress values calculated are valid for the model geometries themselves.

Since both models fall outside the applicability limits for Bijlaard analysis, as presented in Welding Research Council Bulletin 107, there is no guarantee that either result is correct (and there is some likelihood that neither is). Since one would not anticipate exact correspondence between actual solutions for the different geometries, proof of the correctness of results by their numerical identity is tenuous.

It is unlikely that either of the comparison models approximates the actual structure because of the following considerations:

1. The discharge nozzle abuts a stiff ring bolted to a thick, solid-disk, main flange. Even if the casing had no nozzle, this would be regarded as a discontinuity in the casing shell structure. It almost certainly also exerts a major influence on shell stresses from pipe reactions in and around the discharge nozzle.

2. The suction and discharge nozzles are close. This introduces two major departures from model geometry:

a. It negates the uniformity in the shell structure upon which the Bijlaard analysis is based.

b. It introduces interaction stresses in the region between nozzles.

The allowable stresses provided by section III of the ASME Boiler and Pressure Vessel Code are predicated on, and in part justified by, the ability of the analyst using modern analytical methods to accurately appraise stresses. Use of models or methods that do not provide assurance of stress prediction accuracy is, in principle, inconsistent with the use of section III stress limits.

In conclusion, it appears that the pump shell casing geometry should be analyzed by the finite element method to obtain a suitable analysis of stresses.[1]

COMMENT 18.4

The commentary in section A6.3.2.4 states that the thrust coefficient of 1.25 in the formulae for P is appropriate for the main steam line but is not sufficiently high for the feedwater line. A coefficient of 1.9 should have been used.

For saturated water or steam discharge through an idealized no loss nozzle, a thrust value of ~1.25pA (where p is the pressure and A is the area) is predicted based on conservation relations and thermodynamic considerations.

(Westinghouse Electric Corp.)

RESPONSE

For a pipe break in a line initially filled with water that is subsequently expelled by steam, situations may occur (depending on the particular design) that could generate forces larger than 1.25pA. The feedwater line in the PWR plant was believed to be potentially of this character.

Prior to the publication of draft WASH-1400, the vendor presented no evidence that this point had been considered. Lacking specific information, it was felt that a more conservative (i.e., larger) thrust coefficient for the PWR feedwater line should have been used in design.

Subsequently, analyses were performed by the vendor to establish the thrust coefficient appropriate to the PWR plant feedwater line for the case when the steam generator water level drops below the feed ring. This permits high-pressure steam to enter the feedline and accelerate an ever diminishing water mass down the pipe to the break.

It is concluded that an impulse thrust with peak force = 1.35pA is appropriate and conservative for the PWR plant feedwater line. This is based on particular break remote (170 ft) from the steam generator. Breaks less remote develop less thrust. Therefore, the conclusion in section A6.3.2.4 of Appendix X has been modified to indicate that design criteria are satisfied.

COMMENT 18.5

WASH-1400 concludes that it is not certain that LHSIS pump can continue to function during and after impeller deflection of 1.15 in. and that no tests or analyses were performed to provide this assurance.

Calculations show that a momentary interference between the rotating and stationary elements would not be detrimental for a static condition and an interference would not exist at all during the actual operation of the pump.

This conclusion, coupled with the calculated stresses which are shown to be below the allowable stresses, assures design adequacy of the pumps.

(Westinghouse Electric Corp.)

RESPONSE

The drive motor for the LHSIS pump is located about 50 ft above the pump. The drive shaft is encased in a pipe and laterally supported within it at several elevations. The pipe casing, in turn, is braced to the structure. Computations show that during the design basis earthquake the casing will deflect 1.15 in. at the pump end.

When the draft report was written, information had not been provided by the supplier that the pump could continue to operate after experiencing such deflections.

---

[1] It is noted that the supplier intends to perform, and in fact has begun, such an analysis.

Subsequently, a review was performed of the supplier's computations of the deflection of the pump impeller shaft within the pipe and pump casings, together with computations of shaft bearing loads under conditions of maximum deflection. These loads and deflections were derived from a static-g-load analysis for a 3.0 g horizontal acceleration.

The supplier's computations demonstrated that for the conditions investigated:

1. Stator-rotor clearances are not functionally impaired.

2. The maximum shaft bearing load is 370 lb, whereas the bearings have a rated load capacity of 1500 lb.

It is concluded that the methods used in the analysis seem adequate to support this conclusion and the results obtained are reasonable. The analytical approach used by the pump supplier addresses the principal questions concerning the ability of the pump to continue to operate when the pump casing has been deflected 1.15 in. and provides credible engineering assurance that operability will not be impaired by static deflections of this magnitude.

On this basis, the conclusion to section A6.3.3.2 of Appendix X has been modified to indicate that the pump and drive design are adequate. However, since there is no evidence that seismic qualification tests were performed, it has been assessed as adequate with reduced margin.

COMMENT 18.6

The radiation resistance of pump internals, questioned in sections A6.3.3.2 and A6.3.5.1, has been demonstrated and documented.

(Westinghouse Electric Corp.)

RESPONSE

The documents referenced in the detailed comment summarized above have been reviewed. They indicate that substantial irradiation tests have been carried out, and the results appear to be acceptable. However, the documents provided do not contain sufficient information on the tests performed to permit an unqualified assessment of design adequacy. Also, the implied assumption that materials which are radiation resistant under normal ambient conditions will necessarily function as required under operating conditions is questionable. It would be preferable to test the operation of the integral unit after at least the more vulnerable components have been irradiated.

On the basis of the irradiation tests performed, the pump internals have been assessed to be adequate. However, because of the lack of integral tests, the safety margin may be somewhat reduced.

COMMENT 18.7

Appendix X stated that there appeared to be an inconsistency in the results of stress analyses of the accumulator tank nozzles, and the results of the analysis and evaluation performed by the supplier were questionable. Insufficient information existed to assess design adequacy for the stresses during a LOCA.

Westinghouse believes that an incorrect comparison of primary local membrane stresses (σ_L) was made for the loop No. 2 and loop No. 3 accumulators.

(Westinghouse Electric Corp.)

RESPONSE

The vendor has explained the apparent discrepancy reported in draft WASH-1400. Additional documentation of the basis of the analysis, together with useful data and stress results, was also provided. These computations meet the requirements of the ASME Code Section III (including Code case 1607) for Class 3 vessels and adequately demonstrate the ability of accumulator vessel to carry design loads for the faulted condition. Section A6.3.4.1 of Appendix X has been modified appropriately.

COMMENT 18.8

The WASH-1400 draft report stated that the qualification of the sensors and logic cabinets could not be evaluated for seismic and steam environmental exposures with the information available.

Westinghouse believes that the additional information provided with this comment shows that Westinghouse did conduct seismic qualification tests at substantially higher input levels than that contained in Reference 26 of WASH-1400 and the protection equipment was exposed to various environmental conditions.

Based on the above, it is concluded that the PWR components are in fact adequately qualified.

(Westinghouse Electric Corp.)

RESPONSE

With regard to the seismic qualification testing reported, it appears that the instrumentation met accepted criteria. However, since simultaneous biaxial and multifrequency excitations were not included in the qualification tests, the sensors and logic cabinets have been assessed as being adequate with reduced margin.

COMMENT 18.9

The section on seismic loads (section A6.1.1.1) appears incomplete in that current design response spectra were not evaluated for the structures and equipment. In sections A6.1.1.1 and A6.1.2.1, it is stated that the current spectra would increase seismic loads (by as much as a factor of 2). It is not clear what these increases mean relative to the general seismic vulnerability of the 100 plants and what risks are associated with the increases.

(U.S. Environmental Protection Agency)

RESPONSE

Although one may properly infer that changes in seismic design loadings can result from the response spectra currently presented in NRC Regulatory Guide 1.60, one must be careful not to conclude that the overall reported stresses change by the same ratio. This is so because the seismic loading is but one of the many loads considered in determining the overall stress level.

In almost all cases, only critical stresses are investigated and evaluated (i.e., worst case loadings are assumed). For example, the operating basis earthquake (currently one-half the safe shutdown SSE earthquake) is treated as a normal operating load and must be evaluated against the same limits that apply for normal and upset conditions. Worst case loadings would normally be considered and these stresses reported. Thus, in addition to seismic loads, one usually includes loadings from weight, pressure, external applied forces, and the most severe of the upset thermal transients.

Thus, the earthquake load is only a part of total loading considered and accounts only for a corresponding part of the total stress reported. A given percentage increase in the seismic portion of the loading would, in general, produce a smaller percentage increase in the reported total critical stress.

Also the factors of increase (or decrease) in seismic loadings cited in Appendix X are maximum load changes. Load prediction by the response-spectra method is a function of the natural frequency of the structure. Only those structures whose natural frequency corresponds to, or falls within the range of, the frequencies producing the maximum change in seismic load would experience the maximum ratios cited in the report. Other structures are less severely affected.

The question regarding extrapolation to 100 plants is discussed in section 16 of this appendix.

Section 19

Miscellaneous

COMMENT 19.1

Does the containment spray recirculation system (CSRS) provide water to the reactor cavity? From section 2.2.8 of Appendix VIII it appears that the containment spray injection system (CSIS) is assumed not to deliver water to the cavity.

(U.S. Environmental Protection Agency-Intermountain Technologies, Inc.)

RESPONSE

A fraction of both the CSRS and CSIS water reaches the bottom of the reactor cavity. Since the capacity of the CSIS is less than that of the CSRS and since the former operates for a limited period of time, the quantity of water supplied to the cavity due to the operation of the CSIS is much less than that due to the operation of the CSRS.

COMMENT 19.2

The growth rate of reactors may exceed the growth rate of competent designers, operators, maintenance workers, etc.

(Amory Lovins)

RESPONSE

As noted in section 1.9 of the Main Report, the expected improvement in the safety of nuclear power plants depends strongly on the continuing existence of competent and well-supported regulatory and reactor safety research programs and reasonably conservative extrapolation of current practice.

The regulatory program is organized to consider the factors mentioned in the comment. The design of each plant is subjected to a thorough review by the regulatory staff. Criteria for quality assurance programs and safety designs have been established, and frequent regulatory inspections are held to ensure that they are in force. Guides have been published indicating acceptable practices in such areas as personnel selection and training; quality assurance program requirements during design, construction, and operation; preoperational testing requirements; qualification of inspection, examination, and testing personnel; and welder qualification. Furthermore, prior to being authorized to operate a nuclear plant, each operator must pass a detailed examination to demonstrate his competence. He is also periodically retested to ensure that his competence has not deteriorated. The continued existence of such programs should prevent the undesirable events envisioned by the comment.

COMMENT 19.3

The attempt to outline the workings of a large nuclear power plant and what happens in a nuclear accident is inadequate and incomplete. Nor is there an admission that the development of an accident, after its initiation, is little studied.

(Friends of the Earth)

RESPONSE

The study did not attempt to provide a complete treatise explaining the operational principles of a large nuclear power plant; its only purpose was to explore its safety features in potential accident situations in order to provide an assessment of risk. Several excellent texts on the physics and engineering principles of nuclear plants are available. Nuclear reactors and the fission process are described briefly and simply in the booklets entitled Nuclear Power Plants (IB-505) and Nuclear Reactors (IB-507) of the Understanding the Atom series for the layman. (These pamphlets are available from the Energy Research and Development Administration.) In addition, Appendix IX of WASH-1400 provides a description of the basic logic for the safety design requirements imposed on nuclear power plants for the benefit of those not well schooled in reactor safety.

Appendices I, IV, V, VI, VII, and VIII all address in considerable detail the phenomena that might occur after the initiation of an accident and describe how these phenomena would be affected by the operation of various plant engineered safety feature systems.

COMMENT 19.4

The assumption that all fuel stored in the spent fuel storage pool melts on loss of coolant regardless of decay time is highly conservative. This in direct contradiction to the stated objective to perform a more realistic risk assessment.

(Edison Electric Institute)

RESPONSE

In order to determine if accidents outside the core would present any significant contribution to risk, bounding calculations were performed as indicated in Appendix I, section 5. Examination of these calculations revealed that these bounding assumptions presented only a very small contribution to the overall risk (see Appendix V, section 2 and Appendix VI, Section XX). Therefore, detailed calculations to determine the actual extent of damage to stored fuel, given the accidents postulated, were not performed. It should be recognized that this study is an assessment of accident risks in U.S. commercial nuclear power plants. If simple analyses that are clearly conservative show a given item does not contribute to the overall risk, further refined analyses were deemed unnecessary.

COMMENT 19.5

The discussion of "learning curves" in section 2.3.2 of the Main Report to indicate safety will improve with time is facile and unconvincing. The number of fatalities per operation of commercial aircraft has not evidenced increased safety with time. The number of crashes per flight has remained relatively constant.

(Scientists' Institute for Public Information; Amory Lovins)

RESPONSE

As noted in the Main Report, experience from several industries reflects the ability to take advantage of increased knowledge in order to improve safety as a function of time. It is recognized that other industries could be chosen that do not reflect this trend; there are many examples of those that have developed with constant attention to safety and do show an improvement in safety with time. As noted in Appendix IX and in sections 1.9 and 3.3.2 of the Main Report, significant improvements have been made in the safety design requirements for nuclear power plants, in their implementation, and in the applicable codes and standards used in their design as time has progressed. Thus, assuming continued effectiveness of regulatory and research efforts, it is reasonable to expect that the safety of nuclear power plants will continue to improve with time.

Data in Fig. 2.2 of the Main Report are presented in terms of fatalities per 100,000,000 passenger miles. Figure XI 19-1 presents fatal accidents per operation (landing or takeoff) as a function of time[1] for the U.S. air carrier fleet.[2] As can be seen, there is a clear reduction in the fatal accident rate with time. This figure has been added to section 2.3.2 of the Main Report.

COMMENT 19.6

The determination of individual risk as a function of distance from the plant would more correctly show the actual risks to those living within a reasonable distance of a plant.

(AEC Regulatory Staff; Bechtel Power Corp.)

A discussion of individual risk as a function of distance from the plant has been incorporated into Appendix VI, section 13.

---

[1] Data based on information in Tables 2.14 and 10.11, FAA Statistical Handbook of Aviation, Calendar Year 1972, U.S. Department of Transportation, Federal Aviation Administration, April 1974; and Tables 2.8 and 10.3, FAA Statistical Handbook of Aviation, Calendar Year 1973, U.S. Department of Transportation, Federal Aviation Administration, May 1975.

[2] Excludes midair collisions nonfatal to air carrier occupants.

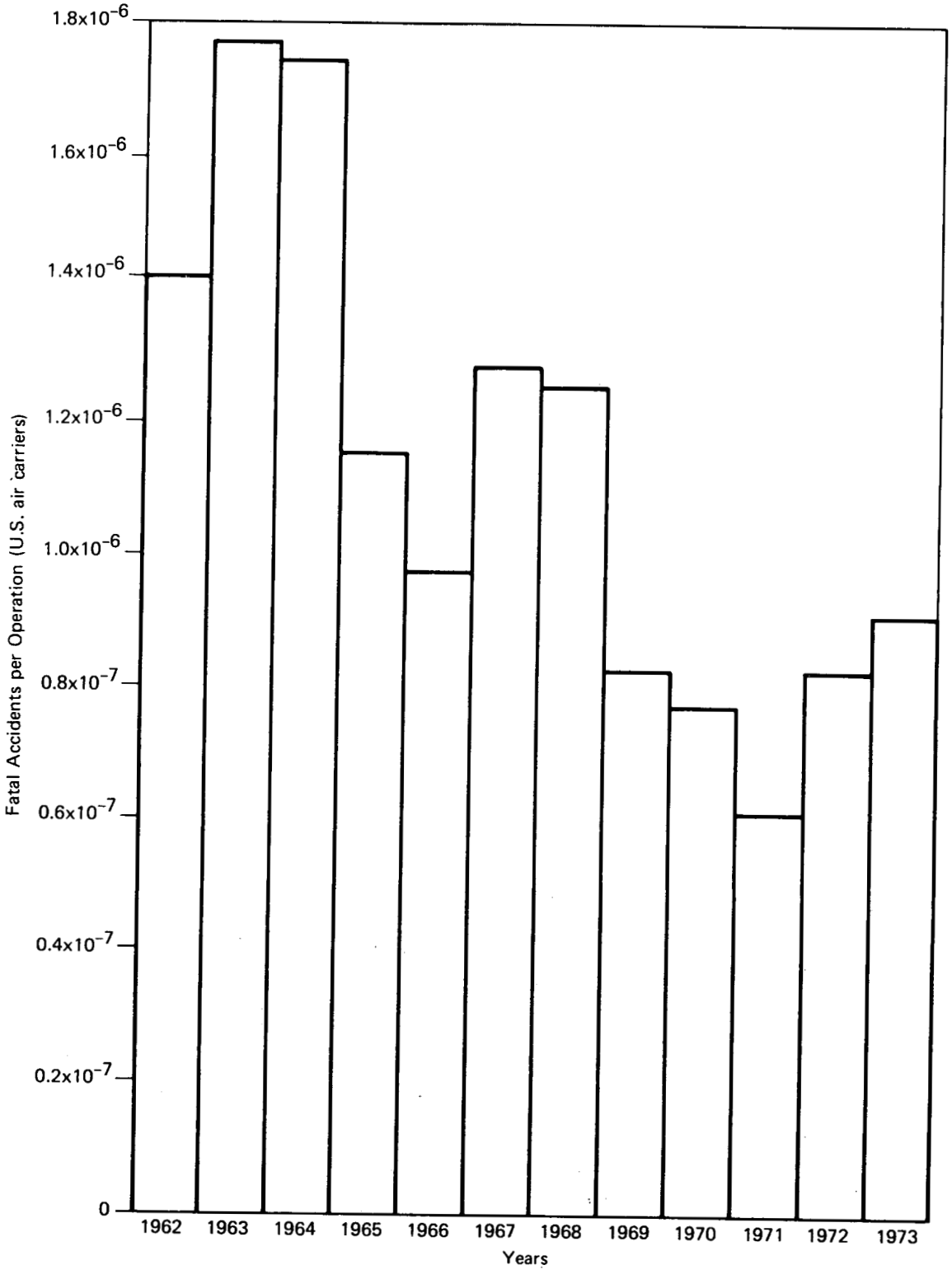


FIGURE 19-1 Fatal Accidents Per Operation (Landing or Takeoff) as a Function of Time for the U.S. Air Carrier Fleet