NUREG/CR-4048
BNL-NUREG-51834

A Methodology for Allocating Reliability and Risk

Prepared by N. Z. Cho, I. A. Papazoglou, R. A. Bari

Brookhaven National Laboratory

Prepared for
U.S. Nuclear Regulatory Commission

NUREG/CR-4048
BNL-NUREG-51834

A Methodology for Allocating Reliability and Risk

Manuscript Completed: March 1986
Date Published: May 1986

Prepared by
N. Z. Cho, I. A. Papazoglou, R. A. Bari

Department of Nuclear Energy
Brookhaven National Laboratory
Upton, NY 11973

Prepared for
Division of Safety Review and Oversight
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN A3728

ABSTRACT

This report describes a methodology for reliability and risk allocation in nuclear power plants. The work investigates the technical feasibility of allocating reliability and risk, which are expressed in a set of global safety criteria and which may not necessarily be rigid, to various reactor systems, subsystems, components, operations, and structures in a consistent manner. The report also provides general discussions on the problem of reliability and risk allocation.

The problem is formulated as a multiattribute decision analysis paradigm. The work mainly addresses the first two steps of a typical decision analysis, i.e., (1) identifying alternatives and (2) generating information on outcomes of the alternatives, by performing a multiobjective optimization on a PRA model and reliability cost functions. The multiobjective optimization serves as the guiding principle to reliability and risk allocation.

The concept of "noninferiority" is used in the multiobjective optimization problem. Finding the noninferior solution set is the main theme of the current approach. The final step of decision analysis, i.e., assessment of the decision maker's preferences could then be performed more easily on the noninferior solution set.

Some results of the methodology applications to a nontrivial risk model are provided, and several outstanding issues such as generic allocation, preference assessment, and uncertainty are discussed.

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

PREFACE

It is important to emphasize that this project is a methodology study of the technical feasibility of allocating reliability and risk. The product of this project, this report, is not a prescription for regulation or licensing. Rather, it is a contribution to the literature in the areas of safety criteria, decision making, and risk analysis. It may be of interest to policy makers and to other interested parties in the nuclear arena who may wish to have this information to enhance their state of knowledge on this particular subject.

The scope of this project did not allow for consideration of the implementation or potential uses of the methods and results presented in the report. However, there is much interest, in the nuclear industry, in how the regulatory agency might choose to use any methods and results in the area of reliability and risk allocation. In addition, the subject of potential NRC usage of the end product of this study was a recurrent topic of discussion with the Steering Group for this project. Thus, while the report itself attempted to remain faithful to the scope of the project, we depart from that scope in this preface and provide here a brief discussion on the subject of usage.

We believe that the concepts, methods, and results of this study will find a number of regulatory uses and applications. Before any usage can be contemplated, some observations are needed on the composition of the "user community".

This community is comprised, from the view of the subject of allocation of reliability and risk, of the existing, individually unique operating plants and plants currently in construction, standard light water reactor plant designs, and advanced or alternative reactor designs. It is also of interest to distinguish plants for which a probabilistic risk assessment (PRA) has been performed from those for which a PRA does not exist.

The report identifies a PRA as a fundamental element of the methodological framework for allocation of reliability and risk. Along with the PRA model of the plant, the notion of cost is included in a systematic way. As described in the report, with the PRA and cost models, the method allows for the gaining of insights that would not be obtained from a straightforward quantification of the PRA models with the existing or expected unavailabilities of system, components, etc. For plants that do not have PRAs, the current method would require, not a complete, quantified PRA, but, for the most part, the system model that is developed from the systems analysis and logic tree development aspects of a PRA.

For operating and constructed plants, a reallocation of reliability and risk would: 1) be done on a plant-by-plant basis; and 2) be limited by cost feasibility since there may be large capital and operating costs associated with a reallocation (retrofit). Alternatively, the methods may be useful in connection with seeking exemptions from existing requirements. One potentially fruitful area for reallocation concepts for operating plants is plant operational practices.

For standard plants and for advanced designs, the methodology can be used and extended to optimize the safety and economics of such future plant designs.

In summary, this report is provided as an initial element from which subsequent ideas and developments can be derived. We welcome comments and suggestions.

ACKNOWLEDGEMENTS

During the course of this work, the authors benefited from many individuals through criticisms, discussions, and suggestions.

First of all, we are grateful to each member of the steering group: G. W. Cunningham, B. J. Garrick, E. P. Gyftopoulos, R. A. Howard, and F. S. Nowlan, who provided us with valuable guidance to the program by offering many constructive criticisms and suggestions.

We are grateful to A. El-Bassioni of NRC for many helpful discussions and for several very useful comments on various drafts of this report.

We also acknowledge R. Frahm and A. Thadani of NRC for their encouragement throughout the work.

We benefited in many ways from our colleagues at BNL: T. Teichmann, P. Farahzad, K. Shiu, N. Hanan, R. Youngblood, W. Pratt, and H. Ludewig. Our discussions with M. Katehakis of SUNY at Stony Brook were also valuable.

We are also grateful to each member of the peer review group: R. deNenfville, J. Hickmann, H. B. Hubbard, R. Jeppesen, W. Kastenberg, G. Sauter, and M. Temme, who reviewed the draft final report and provided us with valuable comments. Comments from the following individuals are also acknowledged: A. G. Adamantiades, G. Apostolakis, A. R. Diederich, S. Kaplan, D. M. Rasmuson, D. C. Richardson, and T. F. Walfinger.

Last, but certainly not least, we acknowledge C. Conrad, D. Miesell, and N. Nelson for their excellent typing during several phases of the report preparation beginning with the first draft report of January 1984.

EXECUTIVE SUMMARY

One of the central themes of contemporary probabilistic risk assessment (PRA) is that the usefulness of PRA derives from the safety insights gained, the identification of plant design and operational vulnerabilities, and the potential role that PRAs may play as safety/risk management tools. It has also been widely said that the "bottom line" risk numbers are the least useful part of a PRA. The dilemma here is that in order to gain the insights, identify the vulnerabilities, and manage the safety/risk, one must go through the process of delineating and quantifying accident sequences and computing various risk indices, i.e., the very nature of the PRA discipline requires that the analyst proceed toward the bottom line.

This report, which presents the methods, results, and conclusions of an initial study on the allocation of reliability and risk in nuclear power plants, contains an approach to probabilistic safety analysis which uses the concepts of bottom line risk indices and the results of the systems and operational evaluations developed in probabilistic risk assessments in a constructively interactive way. The product of this approach is the display of information related to cost and risks of a particular nuclear plant design as a function of the unavailabilities of its constituent components, systems, and structures. Additionally, such information can be displayed as a function of alternative design configurations and/or operational practices by using the methods described in this report.

The study that is reported here is an assessment of the technical feasibility of allocating reliability and risk in a self-consistent manner to various levels of plant performance. Specifically, the analysis addresses the allocation of reliability and risk to reactor systems, subsystems, components, operations, and structures.

It is the conclusion of this study that allocation of reliability and risk is technically feasible. The fundamental elements of the analysis that lead to this conclusion are threefold: 1) a global set of measures of plant performance (top level risk indices or "objective functions") which would be subject to a preference assessment by a decision maker; 2) a model or prescription for relating the global set of measures of plant performance to the specific set of measures of plant performance (system and component unavailabilities, etc. or "decision variables"); 3) a method for deriving a finite, manageable set of self-consistent relations between the global and specific sets of measures.

In this study the first element was identified to be the following global set: core damage frequency, expected acute (or early) fatalities, expected latent fatalities, and the cost of achieving a particular set of values for the first three members of the global set. There were several reasons for choosing the global set at this level of plant performance. First, this set is not plant-specific. Second, this global set is likely to be understandable by the policy-level decision makers. Third, this global set is commensurate with the level of safety criteria that have been promulgated by various parties who have an interest in nuclear power plant operation. We note, however, that our global set of measures are not regarded as prescribed safety criteria

or safety goals. Rather, they are a set of attributes which can be studied, compared and traded off by the decision makers.

Central to our approach is the identification and use of the fourth member of the global set, cost. It was recognized early in this study that the cost of achieving a particular set of values for the first three members of the global set represented a necessary dimension from the point of view of those who must make practical, real world decisions and from the point of view of those who must obtain feasible engineering solutions from the methodology presented in this study.

The second fundamental element, namely, a model which relates the global set to the specific set was identified to be the probabilistic risk assessments (PRAs) which derive top level risk values from plant-specific failures and vulnerabilities. The PRA model is the natural choice for this element because of the abundance of existing PRAs for various nuclear power plants, the level of detail contained in PRAs in the areas of interest to this study, and the potential for enhancing the insights already gained from PRAs by performing the type of study presented in this report.

The third element was identified to be a multiobjective optimization procedure performed on the PRA model with the global set regarded as objective functions. The optimization approach was selected, in part, to reduce the multiplicity of possible solutions to the problem defined by the relation between the global and plant-specific set to a manageable handful and, in part, to obtain the best and most rationally acceptable subset from the multiplicity of solutions. Therefore, the concept of selection of noninferior solutions was introduced; with this concept, solutions which did not yield a relatively favorable value for at least one of the four members of the global set were rejected from further consideration.

The overall methodology has been demonstrated with a nontrivial model. While the model does not represent a complete, particular, realistic power plant situation, it does contain many of the essential features that would be required of an analysis of such a situation. Thus the analysis was conducted for the purpose of investigating technical feasibility and therefore particular features were purposely retained or built into the model in order to test and examine the successes and limitations of the overall methodology. The model is based on a full scope PRA for a BWR/4 MARK-II nuclear power plant. The significant classes of accident initiators and sequences are represented in the model. Dominant cutsets are retained and system dependences are included. In addi-tion, containment performance variables and a seismic accident sequence are studied.

The cost models for the various systems and components are idealized parametric functions, but which nevertheless exhibit the correct intuitive trends for such models. The scope of the project did not allow for the development of realistic component-specific cost functions. However, sensitivity studies were performed on the parametric and functional forms of the cost functions in order to gain familiarity with the implied trends for the global set.

The results of the model analysis are displayed in terms of the set of noninferior solutions to the optimization problem. Thus, for each noninferior solution a set of global values (risk indices and cost) and a corresponding set of plant-specific values (system unavailabilities, etc.) are obtained and displayed. At this point the technical analysis of reliability and risk allocation is complete. It would then be the choice of the decision maker to choose among the noninferior solutions by performing a value tradeoff or preference assessment.

The full display of information (as illustrated in the report) to the decision maker can be a guide in the selection process of those choices which warrant more or less consideration. For example, the full display can indicate the ranges of values for which particular global or plant-specific measures vary rapidly or slowly and thus the incremental value of alternatives can then be gauged by the decision makers.

The subject of preference assessment is briefly reviewed in the report in the context of the allocation problem and a possible approach for future work is suggested.

The report provides a brief study of how to incorporate uncertainty into the allocation procedure and it concludes that a formal technique exists under a set of special assumptions. Less formal approaches, based on sensitivity analyses and error propagation techniques, are also possible.

Some outstanding technical issues related to the allocation problems are:

1) How good are the existing PRA models for the purposes of the allocation procedure presented in this study? The concern is whether hidden dependences, lack of completeness, unrealistic assumptions, etc. would significantly mar the conclusions derived in the allocation procedure. Of course, PRA itself suffers to varying degrees from these shortcomings. Clearly, gross flaws in a PRA model would correspondingly limit the value of the results of an allocation procedure. However, it is not clear at this stage in our investigation whether some of the particular assumptions, methods, and models to which PRA results are significantly sensitive, also lead to correspondingly significant variations in certain results in the allocation problem. This point requires further exploration.

2) Can a useful cost model be formulated? Since the scope of this project precluded detailed investigations of how to formulate realistic cost models, the question must remain open. Further investigations would examine whether appropriate cost data can be gathered on system and component reliability improvement (and decrement) and whether the relevant costs are reflected in the cost models (cost completeness). Further investigation would examine the impact of discontinuous cost-reliability functions on the solutions of the allocation problem.

3) Are uncertainties adequately addressed? In PRA analysis itself, the adequacy of uncertainty analysis is a subject of active investigation. The present report has attempted to address this problem in its discussion of certainty equivalents in Section C.3 and in the approaches to uncertainty that are outlined in Appendix D. Further

investigation is needed in this area and these investigations should consider existing and new developments in PRAs.

4) Are there significant mathematical/computational problems with the current optimization techniques and does software exist or need to be developed to resolve these problems? The report discusses a problem encountered with NOT gates and with better than rare event approximations and their relation to global optimality of the solutions. This problem would need further investigation. In addition, if larger and more realistic models are to be analyzed, then the problem of computational speed may need to be addressed.

5) Are the results and insights obtained from the allocation problem plant-specific or generic? This question does not have a general answer. Clearly, because all U.S. reactors are unique machines, strict and wholesale generic conclusions are not valid. However, some trends and insights may apply to classes or groups of plants. Obvious differences in support system dependences, for example, would tend to preclude strict generic allocation of safety functions and of frontline systems. Nevertheless, some trends (i.e., ranges of allocation) may be discernable upon closer investigation. Of course, the value of this information will depend on its end use and therefore any further investigation ought to be pursued with this in mind.

PART I

MAIN REPORT

1. INTRODUCTION AND BACKGROUND

1.1 Objectives and Scope

This is a report on a program which was performed by Brookhaven National Laboratory (BNL) and sponsored by the U.S. Nuclear Regulatory Commission (NRC). The program is entitled "Guidelines and Criteria for Reliability Allocation". The Office of Nuclear Reactor Regulation (NRR) of NRC is interested in investigating methodologies for qualitative and quantitative reliability allocation guidance.

The objectives of the program are specifically:

1) To examine the technical feasibility of the development of a set of self-consistent reliability allocation criteria for safety functions, plant systems, major components and equipment, and possibly operational practices.

2) To apply the methodology to the development of criteria by providing examples of numerical guidance.

3) To identify problem areas in the allocation procedures.

4) To demonstrate the achievability of the allocated criteria and discuss their flexibility through application.

The NRC has provisionally adopted a set of global safety goals related to the operation of commercial power plants.[1-3] The nuclear industry[4] and other individuals[5,6] also proposed their own safety goals. The purpose of these goals is to provide an easily understandable quantification of acceptable risk. The NRC in particular has adopted two numerical criteria for offsite public health effects, as well as an overall core melt frequency criterion. It is now evaluating potential applications of these numerical safety goals to its regulatory process. One question that arose during this evaluation process is whether the safety goals in their present form are best suited for implementation purposes or whether they should be disaggregated (decomposed) into function/system reliability requirements. It has been argued[7] that such a decomposition would provide a "performance criteria" set in successive tiers of increasing specificity, that could constitute a workable risk management framework for LWRs which is compatible with the needs of reactor designers and operators and is consistent with the top-level quantitative safety criteria. This would be the case because the existence ofreliability goals for plant systems could "lead to a better understanding of the safety importance of the various systems and components and, therefore, holds promise for cost effective improvements".[8] Another argument states that if the objective of the safety goals is to "provide an easily understandable quantification of acceptable risk" then top-level goals would be suit-able; on the other hand, if the objective is to give guidance to designers of plant systems and operating procedures, the criteria at the plant function/system level would serve better.[9] The counter-arguments against the decomposition are variations of the theme that performance criteria at a system level constitute "overregulation". It is argued that what matters is whether a particular plant satisfies the top-level criteria or not; how to satisfy the criteria is not a regulatory function.

This issue bears on the fundamental question of whether the regulatory process should concentrate on the technical details or on the overall performance of the technology. It is noted that presently there exist specific regulatory requirements on the technical details in the design and operation of the nuclear power plants. The examples are the various requirements on the reactor protection system, the decay heat removal function, the auxiliary feedwater system, and the AC emergency power system. Such system performance requirements may or may not lead to risk levels lower than those intended by the standard setter if they are not derived from the overall performance requirements in a consistent manner. The modification or replacement of such sometimes ad-hoc standards at the system level by standards developed by a systematic and consistent allocation (decomposition) of general safety objectives would result in a regulation of the technical details of the technology that is consistent with its overall performance requirements. In addition, it could present additional guidance to the reactor designers and operators on how to satisfy the global safety criteria and, in particular, in cases that involve:

a) Input to backfit decisions,
b) Evaluation of design alternatives,
c) Definition of design and/or operating targets.

In general, the finer the level of the decomposition of the criteria, the more rigid (prescriptive) the regulation and the more the burden of safe design and operation is shifted (in practice) from the plant owner and operator to the regulatory agency.

It is outside the scope of this work to answer the question of how prescriptive the role of regulation should be. However, it is an important policy issue. The objective of this work is rather to answer only the technical aspects of the feasibility of allocation. An approach is, therefore, proposed that suggests the derivation of a regulatory policy on the technical aspects of the technology (system performance requirements) on the basis of a regulatory policy set on the overall performance of the technology. The system performance criteria developed in this way are self-consistent in the sense that "compliance" at the technical level implies "compliance" at the overall performance level.

Also, outside the scope of the present work are the evaluation of any specific set of numerical top-level safety goals (criteria*) and the assessment of value trade-offs among the top-level safety goals. The work does comment, however, on the appropriateness of the particular set of risk indices* as a set of safety/risk evaluators.

1.2 Review of Relevant Work

This subsection presents a brief review of work sponsored by NRC, Department of Energy (DOE), and industry, which is considered to be relevant to the reliability allocation program.

*We use the word "indices" when referring to attributes without numerical values, while the word "criteria" accompanies numerical values.

Following the Three Mile Island accident and an extensive review of auxiliary feedwater systems (AFWS) in light water reactors (LWRs), NRC[10] recommended 10^{-4} to 10^{-5} per demand as an acceptance criterion for AFWS unavailability. The rationale for this recommendation seems to be based on the WASH-1400[11] results and on observations that unavailabilities of the existing good AFWSs excluding outliers of poor reliability estimated by using methods and data in NUREG-0611[12] are in the range of 10^{-4} to 10^{-5} per demand. There appears to be a further consideration, qualitative in nature. That is, WASH-1400 concluded that the contribution to core melt of the extended loss of main and auxiliary feedwater event was approximately equal to the contribution from loss of coolant accidents (LOCAs). Since the challenge frequency for the AFWS is significantly higher than that for the emergency core cooling system (ECCS), the reliability of the AFWS should be higher than that of the ECCS.

Cave and Kastenberg[13] describe quantitative screening criteria for the decay heat removal (DHR) function. In view of the incompleteness and uncertainties in probabilistic risk assessments (PRA) models, notably due to external events such as earthquakes and fires, they suggest a portion (e.g., 60% on the basis of subjective judgment) of the core melt frequency safety goal 1×10^{-4}/reactor year[3] be set aside prior to subdividing the remainder to various safety functions such as the DHR function. In allocating the core melt frequency safety goal, they start with a supposition that "there is no reason to suppose that there is any one unique allocation of the safety goal which will be better than any other".

Knoll[14] describes an approach to optimizing a complex system represented by a fault tree model. The problem is to minimize the system cost under a failure probability constraint. The approach is based on a sensitivity analysis utilizing two types of importance measures: a reliability importance factor and a cost importance factor. The ratio of the two importance factors is used as an index for choosing the component whose reliability is changed first in an iteration. This iteration process is continued until the failure probability constraint is satisfied.

In the field of liquid metal fast breeder reactor (LMFBR) safety, Burdick et al.[15] describe a probabilistic approach to a reactor design optimization problem: Minimizing total plant cost subject to an overall plant reliability constraint. First, lower bounding curves for cost versus system unavailability are determined by using a Monte Carlo approach. These are then input to an intermediate-level minimization problem by assuming that the subsystems are "weakly interacting", i.e., independent. Hartung[16] investigates the role of cost-benefit considerations and a priori risk criteria as determinants of core disruptive accident (CDA)-related safety criteria for large LMFBRs. He develops a methodology which is formulated as an optimization problem: Minimizing energy generation costs subject to the constraints of an a priori risk criterion and a cost-benefit criterion. Gokcek et al.[17] describe a similar risk allocation model of a constrained nonlinear programming problem: Minimizing reliability improvement cost subject to maximum risk criteria. Hurd et al.[18] also describe, for design options studies, a risk allocation model of a constrained integer nonlinear programming problem: Minimizing total costs of research and development and of reliability improvement subject to risk criteria.

It is noted that the optimization problems treated in Refs. 14 through 18 are of the single-objective programming approach whose limitations and drawbacks will be discussed in Section 2 and Appendix A.

1.3 Steering Group and Peer Review Group

A five-member steering group* of both nuclear and non-nuclear expertise was formed to provide general guidance to the program. Some of the objectives defined for the steering group are:

i) To bring into the nuclear arena ideas and experiences from other fields.

ii) To count on the group membership expertise to define direction which enhances the practicality and effectiveness of the program.

iii) To evaluate the feasibility and applicability of the end product of the program.

During the course of the work, the authors and the NRC staff cognizant of the program had fruitful discussions with the Steering Group members. We presented to them two interim reports for review and comments and held two meetings for discussions. Appendix E includes the comments made by individual members of the Steering Group. Although the comments are reflected in appropriate sections of this report, our discussions addressing the comments are also included in Appendix E.

A seven-member peer review group with experience in fields broadly related to the program was also formed in order to obtain comments on the draft final report.

We presented the draft final report to the steering group and the peer review group and also held a workshop for discussions.

1.4 Principles and Characteristics of the Proposed Approach

As is stated in Section 1.1, the general objective of this work is to examine the technical feasibility of the development of a set of reliability criteria for plant systems/major components consistent with a set of top-level safety goals.

The first step in our work was to examine the set of top-level (global) risk indices presently under evaluation, for appropriateness and completeness. The two health indices (acute and latent fatalities) and the probability of core damage were considered as appropriate global risk indices. Very early in our work, however, it became apparent that a rational and meaningful set of reliability criteria could not be developed unless cost considerations were introduced into the thought process. It was also recognized that, since different levels of safety criteria are attainable at different costs, a solution to the problem will not be complete without a preference assessment (value trade-offs) among the various risk indices. These two points are related to the fundamental question of whether "standard setting" constitutes

*Appendix E gives the names and affiliations of the steering group members.

a better way of regulation than "case-by-case decision making". Decision making procedures attempt to order options according to relative attractiveness; standards simply categorize them as "acceptable/not acceptable".[19] The present state of regulation is a mixture of these two ways of regulation in that it employs a case-by-case review on alternatives (plants) that have been already designed and built according to a set of design standards. This work does not attempt to resolve this issue, but it does take the technical position that the set of global risk indices, whether used as a basis for developing standards or used as "performance indices" for decision making purposes should include cost considerations. Furthermore, it is claimed, that a preference assessment on the various safety and cost measures is a necessary step for a meaningful regulatory procedure based on either approach. The preference assessment is, however, a basic policy question and this report simply suggests a procedure for addressing it.

The fundamental elements of the approach proposed in this study are threefold: 1) a global set of measures of plant performance (top level risk indices or "objective functions") which will be subject to a preference assessment by a decision maker; 2) a model for relating the global set of measures of plant performance to the specific set of measures of plant performance (system and current unavailabilities, etc. or "decision variables"); 3) a method for deriving a finite, manageable set of self-consistent relations between the global and specific sets of measures.

In this study, the first element was identified to be the following global set: core damage frequency, expected acute (or early) fatalities, expected latent fatalities, and the cost of achieving a particular set of values for the first three members of the global set. There were several reasons for choosing the global set at this level of plant performance. First, this set is not plant-specific. Second, this global set is likely to be understandable by the policy-level decision makers. Third, this global set is commensurate with the level of safety criteria that have been promulgated by various parties who have an interest in nuclear power plant operation. We note, however, that our global set of measures are not regarded as prescribed safety criteria or safety goals. Rather, they are a set of attributes which can be studied, compared and traded-off by the decision makers.

The second fundamental element, namely, a model which relates the global set to the specific set was identified to be the probabilistic risk assessments (PRAs) which derive top level risk values from plant-specific failures and vulnerabilities. The PRA model is the natural choice for this element because of the abundance of existing PRAs for various nuclear power plants, the level of detail contained in PRAs in the areas of interest to this study, and the potential for enhancing the insights already gained from PRAs by performing the type of study presented in this report. Consequently, the methodology is characterized by the same advantages and limitations that characterize the PRA models. All aspects of plant behavior that are included in the presently available PRA models; e.g., dependences, recovery probabilities, test and maintenance characteristics, can be taken into account. On the other hand, the methodology does not answer fundamental "incompleteness" questions (such as the contribution to risk from sabotage or unforseen accident sequences) or address aspects of the probabilistic behavior of the plant that are not included in the state-of-the-art PRA models.

The third element was identified to be a multiobjective optimization procedure performed on the PRA model with the global set regarded as objective functions. The optimization approach was selected, in part, to reduce the multiplicity of possible solutions to the problem defined by the relation between the global and plant-specific set to a manageable handful and, in part, to obtain the best and most rationally acceptable subset from the multiplicity of solutions. Therefore, the concept of selection of noninferior* solutions was introduced; with this concept, solutions which did not yield a relatively favorable value for at least one of the four members of the global set were rejected from further consideration.

In essence, the proposed approach transforms the problem of determining a set of reliability criteria into one of determining an "optimum" design. The optimum (noninferior) designs are determined by considering simultaneously the multiple global risk measures and the cost. The reliabilities that characterize the components of these noninferior designs constitute sets of reliability criteria. In that sense, the proposed approach is a "forward" or "bottom-up" approach.

The methodology can be divided into two steps that separate the technical issues from the policy issues. The first step which is mainly developed in this work consists of the determination of a set of noninferior solutions (sets of low-level criteria) that does not require a preference assessment. The second step further reduces the set of noninferior solutions determined in the first step through the establishment of value trade-offs among the top-level risk measures and the cost. This second step is outside the scope of this work.

1.5 Organization of the Report

The report is presented in two parts: the Main Report and the Technical Appendices. The main report summarizes the proposed methodology, its applications, and its conclusions, while the technical appendices provide the technical details involved.

Section 2 of the main report provides general discussions of the problem and briefly describes the framework of the methodology.

Section 3 provides the results of an application of the methodology to a relatively complex probabilistic risk assessment (PRA) model, and discusses advantages of the approach taken in the methodology over other approaches.

Section 4 provides insights gained from and conclusions of the study with recommendations for future directions of the subject program.

Appendix A of the technical appendices first provides general discussions on the idea and the implications of reliability allocation and performance criteria. It then discusses the need for cost considerations. It next provides the basic elements of an allocation problem and describes the proposed decision-theoretic methodology in detail followed by simple examples to illustrate the methodology.

*The term is formally defined in Section 2.4 and in Appendix A.

Appendix B provides nontrivial applications of the proposed methodology to an existing PRA model and discusses the results, including sensitivity studies.

Appendix C provides a brief discussion on the preference assessment of the decision maker and reviews the decomposition method which appears to be a useful approach to complex decision problems. It also discusses the use of certainty equivalents.

Appendix D addresses the issue of uncertainty and provides several approaches to incorporating or reflecting uncertainties into reliability allocation.

Appendix E provides a two-level decomposition approach to a particular problem in which component reliabilities are allowed to take only discrete values.

Finally, Appendix F includes the written comments made during the course of this work by individual members of the Steering Group and the discussions provided by the authors of this report.

2. METHODOLOGY DEVELOPMENT

The choice between two sets of low-level criteria implies or requires a choice between two possible different sets of top-level criteria. Such decision making problems in which there are several conflicting objectives can be addressed by the techniques of multiobjective optimization. There are many examples of problems with several conflicting objectives, particularly in the public sector, which must deal with society's objectives. Furthermore, many of the objectives are intangible and noncommensurable. The usual single-objective approach to this type of problems requires that all attributes of objective functions be measurable in terms of a common unit, e.g., in dollars as in cost-benefit analysis. Thus, the single-objective approach at best masks the decision maker's role of making value judgments or even worst transfers the decision maker's role of making value judgments to the analyst. The multiobjective optimization approach adopted in this work, however, pursues a full exposition of the problem and explicit consideration of the relative values of all alternatives and presents them to the decision maker. By systematically investigating alternatives, the range of choice and the relationship between alternatives and the trade-offs of the objective functions are identified. In this way, the role of making value judgments will remain where it belongs, that is, with the decision maker. Treatments on the subject of multiobjective programing can be found in Refs. 20 and 21. It is also noteworthy that this approach was considered in nuclear power plant siting problems.[22]

In the context of a risk related decision making, the multiobjective optimization problem is formulated as follows.

2.1 Objectives and Attributes

The first step in a decision making problem is the definition of a set of objectives that each alternative is trying to satisfy and for each objective the definition of an attribute or measure of effectiveness. An attribute provides a quantitative measurement of the degree to which the corresponding objective has been achieved. For the purposes of this work four attributes are considered:

1.	Core Damage Frequency	C_d	$(= Z_1)$
2.	Expected Acute Fatalities	A	$(= Z_2)$
3.	Expected Latent Fatalities	L	$(= Z_3)$
4.	Reliability Cost	G	$(= Z_4)$

(2.1)

The first three attributes are included because they constitute the basis* of the various proposed "safety goals" and the final risk measures calculated in current PRAs. The need for the attribute "Core Damage Frequency" in addition to the attributes for the health effects stems from the fact that the implications (consequences) of an accident resulting in core damage go

*Some safety goal formulations express health effects in terms of risk to an individual while other formulations refer to societal risks.

beyond the specific health effects and economic consequences of the accident. Even if the health effects are negligible, such an accident will probably have a significant impact on the entire nuclear industry. The impact of core damage, therefore, cannot necessarily be measured in terms of the other attributes or evaluation indices of the alternative nuclear power plant designs. It rather has a "value" of its own and consequently it must be included as an attribute. It is thus a non-redundant[23] attribute. The attribute "Core Damage Frequency" is also non-redundant with the attributes A, L in a mathematical sense. This means that although there exist functional relationships among the three attributes C_d, A, and L, the value of any one attribute is not uniquely determined by the values of the others.

The use of expected values as measures of effectiveness is discussed in Section C.3 of Appendix C.

The introduction of the fourth attribute is necessary, since economic considerations are important in any (even regulatory) decision making concerning power generations from nuclear power plants. In the absence of economic considerations the problem would be equivalent to answering the vague question of "how safe is safe enough". Trying to answer this question in isolation of economic considerations could lead to answers which are not supported by practical considerations. If there were no constraints on the achievability of the various system reliability levels, we would choose the solution which results in the lowest possible consequences. In the limit, this would have implied zero consequences achieved through perfect system reliabilities. Of course this is not possible, since a) a particular level of system reliability is achieved through the expenditure of resources and b) there are technological constraints on the achievable levels of system reliability. The "cost" implied by a particular reliability level is, therefore, a necessary ingredient in our problem, and the reason for seeking a solution other than that obtained by reaching the highest (mathematically or technologically) achievable system reliabilities. These cost considerations are further elaborated in Appendix A.

2.2 Plant Model

In the second step the nuclear power plant is considered to consist of a logical interconnection of a number of "elements" each of which is characterized by an unreliability level x_i. The elements can be of a varying degree of detail depending on the level of decomposition of the plant model (e.g., safety functions, systems, trains, components). The logical interconnection of the elements is described by a mathematical model that expresses the four attributes mentioned in Section 2.1 as functions of the unreliability levels x_i. Denoting a specific set of x_i's as $\underline{x}$ the logical model of the plant consists of a set of four equations:

$$Z_i = f_i(\underline{x}) \qquad i = 1, 2, 3, 4 \qquad (2.2)$$

where Z_i, i = 1, 2, 3 are provided by a PRA model and Z_4 is determined by reliability cost functions.

The details of a PRA model are given in Appendix A. We use the terms "unreliability" and "unavailability" interchangeably and it is not crucial,

for the purposes of the work, to distinguish them in a strict mathematical sense. They collectively refer to the various failure probabilities such as passive and active failures of components, failures on demand, failures to run successfully after starting, failures to recover failed components, human errors, operation and maintenance procedures, containment performance characteristics, component dependences and scenario dependent unreliabilities. The methodology applications presented in Section 3 and Appendix B of this report includes examples of all these elements of the PRA.

The current PRA models do not take into consideration the costs related to the reliability of the plant. This is because the PRA is used primarily as an evaluation methodology of a given plant.* If the PRA model is to be used in a methodology that compares alternative reliability allocations of the plant, the cost involved becomes an important element as discussed in Subsection 2.1. The type of cost of interest for this study is that associated with achieving a particular level of reliability for safety related systems.

If the cost of achieving the unreliability x_i of the i^{th} component is denoted by $g_i(x_i)$ then the expression used in this study for the total cost (Z_4) is

$$Z_4 = \sum_{i=1}^{n} g_i(x_i) \tag{2.3}$$

where n is the number of components.

The cost functions $g_i(x_i)$ include all technologically feasible unreliabilities x_i for component i. In that respect "cost" is a measure of the "degree of difficulty" in achieving a specific level of unreliability.

The usual assumption that cost is a monotone increasing function of unreliability (or equivalently that cost is a monotone decreasing function of unreliability) is a logical one (see the details in Appendix A) and it is incorporated in the methodology proposed in this work. It may be possible that following the application of the methodology a good designer can come up with a new idea that will result in a component with an unreliability at a cost lower than that predicted by the cost function. In that case, the methodology must be reapplied in the light of the new information.

For the purposes of demonstrating the methodology, it suffices to consider only the cost associated with achieving the various unreliabilities [see Eq. (2.3)]. All other costs associated with the nuclear power plant or a particular accident need not be considered until a realistic preference assessment is made. These additional costs are important when trade-offs among the various attributes are to be made.

*There is, however, a growing interest in utilizing PRA results for cost-effective plant modifications, e.g., Ref. 24.

2.3 Decision Space - Alternatives

In the third step of the methodology, the set of all the alternatives to be evaluated - the decision space - is defined. The proposed methodology is "forward" in nature in the sense that it starts with all possible different realizations of a nuclear power plant and then it proceeds in evaluating these alternatives in terms of the top level criteria or attributes. There are two major ways of generating alternatives. One is to consider alternative designs (or component configurations). There might be a single configuration or several configurations (designs) under consideration. The other is to consider - for a given configuration - different component unreliabilities. The component unreliabilities can take a single value, discrete values, or continuous values in a given range. Consequently, there are six possible combinations of component configurations and component unreliabilities that correspond to the six types of decision spaces shown in Table 2.1.

The methodological concepts developed in this work are valid for the five non-trivial types of decision spaces shown in Table 2.1. The particular mathematical techniques of multiobjective optimization presented here are, however, applicable only to decision-space types 1 and 2. The particular applications of the methodology presented in Section 3 and Appendix B are based on decision-space type 1. The authors see, however, no fundamental problem in extending the approach to decision-space type 2. Problems involving decision-space types 3, 4, and 5 require different mathematical techniques (e.g., discrete optimization techniques) than those presented in Appendix A. Appendix E provides a two-level decomposition approach to a particular problem of decision-space type 4.

It is noteworthy that the unreliability of a component can change in a continuous way without any hardware change. This is possible, for example, by a change in the operating conditions; e.g., test and maintenance policies. It is also possible to change the configuration of a system (different design) and yet the only effect of this change in the PRA model is through the change in its unreliability value.

Mathematically, the decision space is the set of all technologically feasible realizations of the vector $\underline{x}$ (where the dimensionality of $\underline{x}$ is equal to the number, n, of the decision variables x_i. A given design (component configuration) with continuous component unreliabilities corresponds to a region in the n-dimensional space R^n. A given design with discrete component unreliabilities will be represented by discrete points $\underline{x}^j$, where j is the j^{th} permutation of the various discrete values of the x_i's.

Examples of decision spaces are depicted in Figures 2.1 and 2.2 for the two-dimensional case. Figure 2.1 depicts the decision space for the case of a new plant/design. The feasible solutions include points characterized by higher unreliabilities - northeast corner of F_d. Because this is the case of a new design (with starting point $\underline{x}_0$), all feasible alternatives including higher unreliabilities than the initial design $\underline{x}_0$ are considered since there is the possibility that the lower cost of these alternatives might offset the possible increase in the other attributes.

Figure 2.2 depicts the decision space for the case of an existing plant. The feasible alternatives now include only the points with lower unreliabilities than the existing level $\underline{x}_0$ since it is highly improbable that the unreliability of an existing component can be increased with an associated cost reduction.

Table 2.1 Decision Space Types

	Unreliabilities		
Configurations	Continuous	Discrete	Single Valued
Single	1	3	-
Several	2	4	5

2.4 Multiobjective Optimization - Noninferior Subspaces

In the fourth step of the methodology, the alternatives established in the third step are evaluated and the "best" solution is selected. This choice is a decision problem.

In a mathematical formulation, this problem is equivalent to choosing the most preferred point out of all the points of the feasible space F_d. Each alternative is evaluated in the four attributes established in the first step of the methodology. These four attributes define a four dimensional Euclidean space called the outcome (or consequence) space. To each point $\underline{x}$ of the decision space there corresponds a point $\underline{z}$ in the outcome space determined by the plant model. In other words, the PRA model maps the feasible space F_d to the outcome space R_0. A pictorial representation of this mapping is given in Figure 2.3 for the two-dimensional case. The problem then reduces to one of choosing the point $\underline{z}$ in R_0 that is the most preferred. Since, in this application, less in each of the attributes is more preferred, it is straightforward to choose between two points $\underline{z}^*$ and $\underline{z}^0$ for which we have that

$$z_i^* < z_i^0 \qquad (i = 1, 2, 3, 4) \tag{2.4}$$

with the inequality strictly holding for at least one i. Outcome $\underline{z}^*$ is clearly preferred to outcome $\underline{z}^0$. The same is true for the alternatives $\underline{x}^*$ and $\underline{x}^0$ that result in the outcomes $\underline{z}^*$ and $\underline{z}^0$, respectively. Eq. (2.4) is usually summarized by saying that point $\underline{z}^0$ (or $\underline{x}^0$) is "dominated" by point $\underline{z}^*$ (or $\underline{x}^*$), or that point $\underline{z}^0$ is "inferior" to point $\underline{z}^*$.

A first step to solving the decision problem could, therefore, be the exclusion of all dominated points in the set R_0 and consequently of all the dominated points in the set F_d from being viable alternatives. The points in F_d that remain after exclusion of all dominated points form the so-called "efficient frontier" or "noninferior set" N_d. The definition of the "noninferior set" is graphically depicted in Figure 2.3 for a two-dimensional case.

The noninferior set can be found by the solution techniques of multiobjective optimization that are described in Subsection A.3.3. There are several techniques for determining the noninferior set N_d. In the case of continuous decision variables this determination is equivalent to fixing all the outcome variables but one then solves a single objective optimization problem with this particular variable as the objective function. The solution provides a single point in the set. Changing the values of the fixed outcome variables and resolving the optimization problem provides another point, and so on. The techniques developed in this work are applicable to decision spaces of types 1 and 2 (see Table 2.1, Subsection 2.3).

If there are only a few alternatives (discrete decision space F_d) then the generation of the noninferior set by enumerating the design alternatives is probably better than a mathematical optimization over continuous approximations to reality. However, in most of the discrete cases (decision space types 3, 4, and 5) the number of alternatives might be extremely large so that a continuous approximation of F_d or a more efficient discrete-optimization technique could be still necessary. For example, there were 33 distinct post-TMI system design modifications proposed by NRC staff for BWRs. The implied alternatives [more than $8 \times 10^9 = \sum_{i=1}^{33} \binom{33}{i}$] are too many for exhaustive enumeration.

2.5 Preference Assessment

Comparison between any two points in the noninferior set is no longer straightforward, since some of the attributes will have more preferred values for one point while others will have more preferred values for the other point. To compare two points of the noninferior set, preferences over the values of the attributes should be established.

The establishment of value tradeoffs (preferences) among the attributes of the decision problem is necessary for its ultimate resolution. The noninferior space N_d could be too wide to offer meaningful guidance both to regulators and to designers/operators of nuclear power plants. Any restriction of this space to a smaller range or to one point must be accomplished in the corresponding noninferior outcome subspace N_0 and it requires the explicit or implicit establishment of value tradeoffs. The preference assessment is also important for another technical reason. The assessment of the most preferred point in the noninferior set of solutions could be greatly simplified if the preferences have been assessed in advance. This means that the establishment of the noninferior set is not necessary anymore, and that the most preferred point can be established directly. The technique of the multiattribute utility theory[23] or the "decomposition" technique[25] suggested by one of the members of the Steering Group could be used for this purpose. Furthermore, the suitability of the form of the attributes (i.e., expected values) as performance evaluators depends on particular characteristics that the preference structure might exhibit (see Section C.3).

The importance of the preference assessment for the ultimate resolution of the decision problem and the effect that it might have on the methodology notwithstanding, answering the preference question is equivalent to establishing regulatory policy and as such it is outside the scope of this study. It

was tried, therefore, to separate the technical issues from the policy issues of the problem. Every effort was made, however, to stress the importance and the impact of preference assessment issues to the extent that the resources of the project permitted (see Appendix C).

2.6 Potential Uses of Noninferior Subspaces

The proposed methodology is a decision-theoretic approach and uses the techniques of multiobjective optimization to identify the set of noninferior solutions N_0 in the outcome space and the corresponding set N_d in the decision space. It is noteworthy that this procedure constitutes a "bottom up" or "forward" approach in the sense that it considers each and every possible "plant design" and assesses which of them can be discarded on the basis of being dominated by another design. The methodology, this way, allows and at the same time provides for more alternatives to designers/operators of nuclear power plants than a specific set of safety goals would make possible. This is due to a) the "forward" nature of the methodology - it starts with every feasible alternative and b) the unrestricted range of top-level safety criteria (attributes) that include the economic dimension.

In practice, the proposed methodology could be implemented as follows:

a. Define the functions f_i in Eq. (2.2) using a PRA model corresponding to the logical configuration(s) for the plant at a given level of resolution.

b. Define feasible points $\underline{x}$. This (along with the configuration) is equivalent to defining the space F_d.

c. Use the techniques of mathematical programming to establish points in the set of noninferior solutions.

d. Tabulate the points of the noninferior set as shown in Table 2.2.

Tables in the form of Table 2.2 can be used to communicate the results to decision makers and facilitate the preference assessment. The points of the noninferior set will be tabulated according to the value of the attributes. One tabulation will result by keeping the frequency of core damage constant. Thus, first we tabulate the points that result in the highest frequency of core damage say z_1°. Next, we tabulate points that result in lower frequency and so on until we tabulate the points with the lowest level of core damage frequency - z_1^*. Perusal of these tables by decision makers would facilitate their study of the other three attributes z_2, z_3, and z_4. The results of the example problem indicate that if z_1 is held constant then attributes z_2 and z_3 vary in the same direction. That is, for two points $\underline{z}'$ and $\underline{z}''$, if $z_1' = z_1''$ then $z_2' > z_2''$ implies $z_3' > z_3''$. If this is always the case, even with a small variation in z_3, the choice problem reduces to assessing preferences between two attributes (z_2 - acute fatalities and z_4 - cost) conditional on a certain level of attribute z_1. In this way, a number of points can be dropped out from the original table. The points of the noninferior set can then be retabulated in decreasing order of the attribute z_2 and the process repeated. Finally, a reduced table of noninferior points will result.

Examination of this table will establish ranges within which each "decision variable" x_i - "component unreliability" - lies. If these ranges are narrow enough they can probably be established as design "aspirations" towards which a specific plant would be designed (new plant) or backfitted (existing plant). In particular, for existing plants realistic and feasible backfitting options would be examined on the basis of the established unreliability "aspirations" and the existing systems.

The use of the noninferior sets are depicted graphically in Figures 2.4 and 2.5 for a new plant and an existing plant, respectively. The difference between these two cases is that for an existing plant only improvements in the component unreliabilities at a certain cost are considered as feasible alternatives. In both cases, the objective is to bring the initial design $\underline{x}'$ within the noninferior set N_d. Any other alternative solution $\underline{x}''$ can be checked for acceptance by examining whether it belongs to the noninferior set or not.

In general, the proposed methodology is useful (efficient) whenever there are many feasible alternatives. Otherwise, a PRA and inspection of its results plus judgment could suffice.

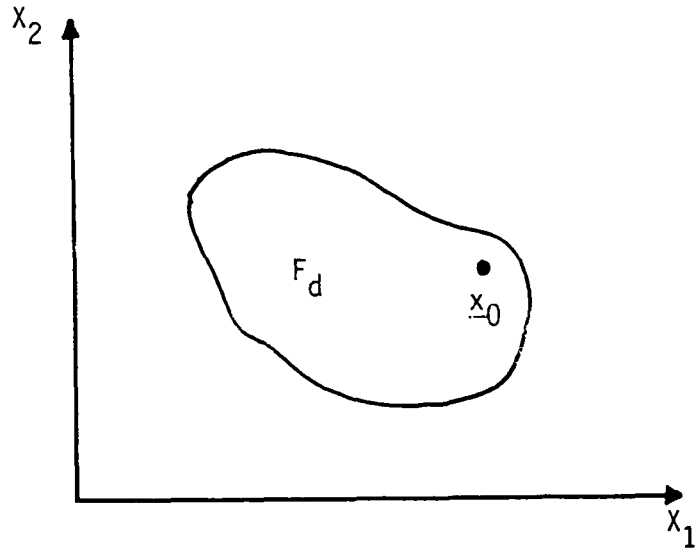


Figure 2.1 Decision space for a new plant with initial design $\underline{x}_0$.

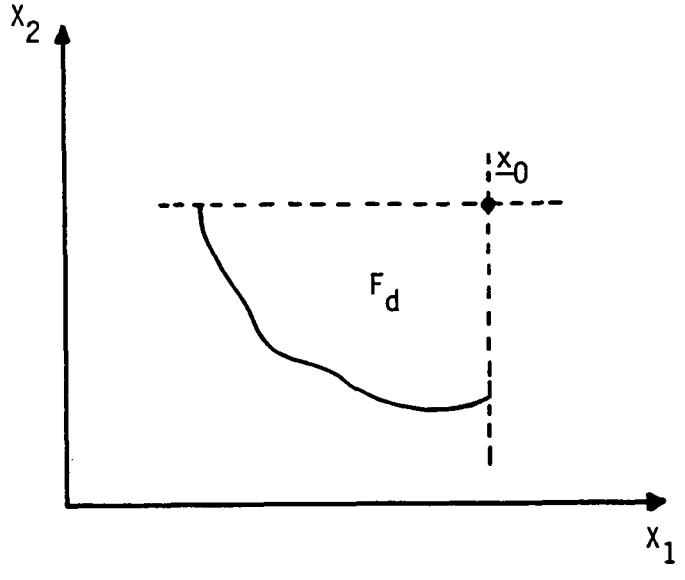


Figure 2.2 Decision space for an existing plant with design $\underline{x}_0$.

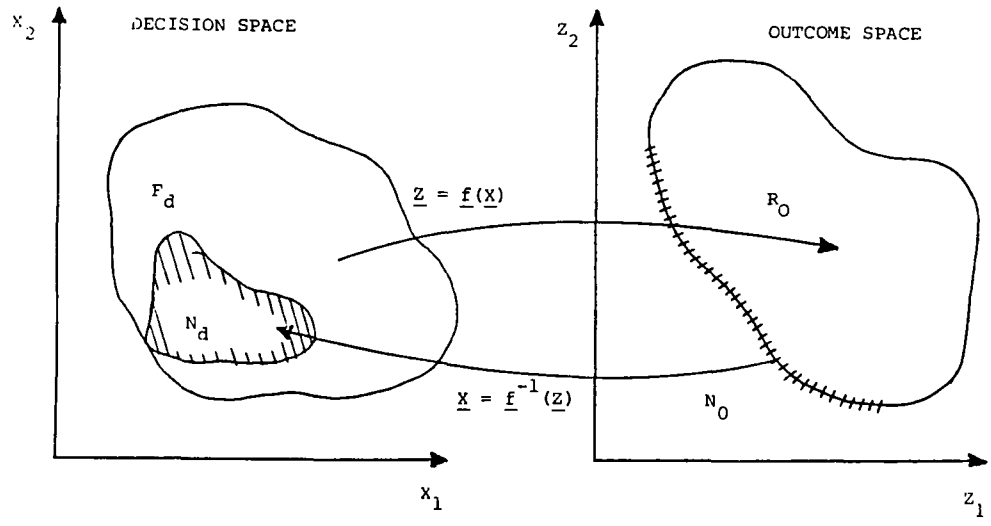


Figure 2.3 Mapping of decision space into outcome space.

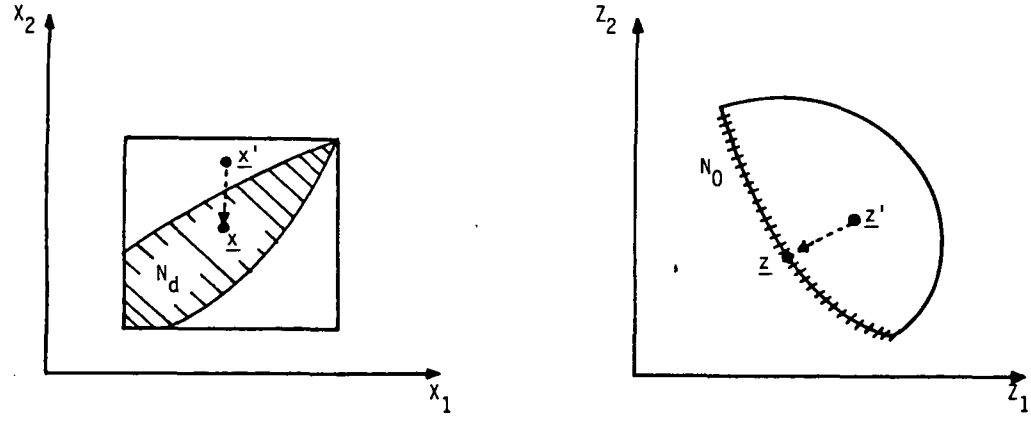


Figure 2.4 Use of noninferior subspace for a new plant.

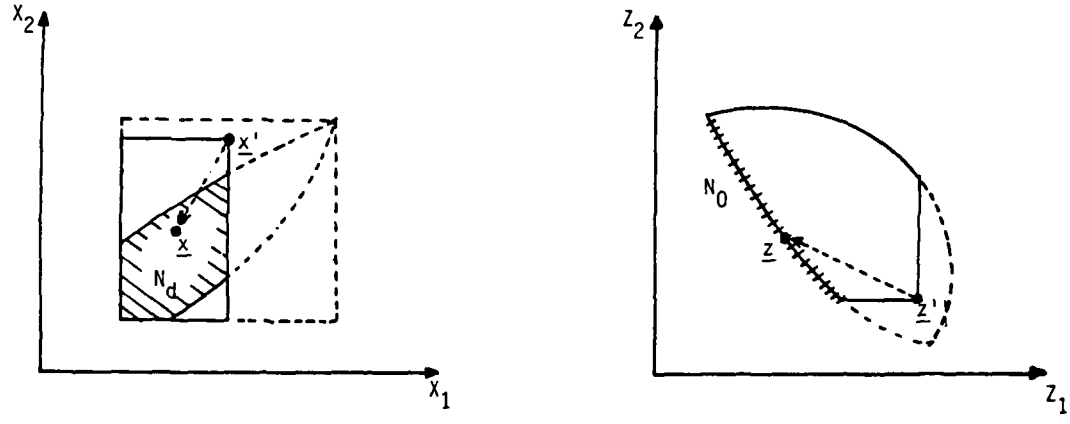


Figure 2.5 Use of noninferior subspace of an existing plant.

Table 2.2 Noninferior Points in Outcome (Consequence) and Decision Spaces

Points		1	2	. . .	k
Outcomes	$z_1(C_d)$ $z_2(A)$ $z_3(L)$ $z_4(G)$				
Unavailabilities	x(1) x(2) . . . x(N)				

3. METHODOLOGY APPLICATION

This section presents applications of the methodology to a complex PRA model. The model was taken from the review[26] of LGS-PRA.[27] Although the PRA model used in the section is not a detailed, full-blown model, it represents a good approximation to a complete PRA model and contains most of the aspects that would be of interest in a demonstration of the proposed methodology. We caution, however, that the model analyzed here does not, and is not, intended to represent the Limerick plant. Thus, no conclusions should be directly drawn with regard to the safety or operation of that specific plant.

In the first application, the noninferior subspace was developed for a set of decision variables that includes only supercomponent unreliabilities for systems that affect the accident sequences up to core damage. This base model was then extended to include a seismic sequence and also to include containment performance parameters in the decision variables. This extended model demonstrates the feasibility of incorporating external events and containment performance within the allocation methodology.

Table 3.1 gives a list of the decision variables while Table 3.2 gives their corresponding ranges (i.e., it defines the feasible space F_d). The first 19 variables in Table 3.1 were used in the base model and all 22 in the extended model. Further details for the models are given in Appendix B.

3.1 Results and Discussion - Base Model

The results of the base model are presented in Tables 3.3 through 3.8 in this section while the results of the extended model are presented in Appendix B.

The set of noninferior solutions represents a hypersurface in the four dimensional space (C_d, A, L, G). The intersection of this surface with a hyperplane corresponding to a constant value of C_d [i.e., (C_d = const, A, L, G)] is a curve in the three dimensional space (A, L, G). The "projection" of this curve on the (A, G) plane gives a trace which is depicted in Figure 3.1 for several values of C_d. Figure 3.2, on the other hand, depicts the projection of the (C_d = const, A, L, G) curves on the (L, G) plane.

Examination of these traces leads to the following three general observations:

i) Each trace, for example on the (A, G) plane, Figure 3.1, is characterized by two extreme points (lower and upper limits). For the C_d = 10^{-3}/ryear case, for example, these two extreme points are points A_1 and A_6. This means that it is not possible to lower the reliabilities (and hence the cost of the plant) and increase the expected acute fatalities more than the values corresponding to solution A_6 without increasing at the same time the frequency of core damage. On the other hand, it is not possible to lower the unreliabilities (and hence increase the cost of the plant) and decrease the expected acute fatalities more than the values corresponding to solution A_1 without decreasing at the same time the frequency of core damage. Recall that in the base model the containment characteristics are held constant.

ii) The acute and latent fatalities vary in the same direction.* That is, an increase in acute fatalities is always associated with an increase in latent fatalities. The relative change in the acute fatalities is, however, larger than that of the latent.

iii) With the exception of X(1) and X(2), the rest of the decision variables do not vary considerably when the core damage frequency is held constant. The two variables that vary correspond to the unavailabilities of the reactor protection system and the standby liquid control system that control the probability of an ATWS. The variation in the latter probability explains the variation in the acute and latent fatalities.

As discussed in Section 2.6 the following procedure can now be followed. The first step consists in choosing one solution as most preferred within each group with constant core damage frequency. A preference assessment is necessary now. At this point, the choice could be rather easy and it involves only an informal preference assessment. For example, we can ascertain by examining the two extreme points in each group (e.g., B1 and B5 in Figures 3.1 and 3.2) that the decrease in the acute and latent fatalities is not significant enough to offset the corresponding increase in the cost. Consequently, from each group of solutions we retain only the one that implies the lowest cost. These solutions (A6, B5, C8, D8) are tabulated in Table 3.3. A choice among these four solutions would require a more involved preference assessment. We can, however, examine the implied ranges of unreliabilities to see whether any conclusions can be drawn before proceeding with the selection of the best solution.

The ranges of unreliabilities that are suggested by our preliminary screening are given in Table 3.4. These ranges can then be further grouped into three categories as shown in Table 3.5. Systems characterized by "narrow" or "very narrow" ranges of unreliabilities have their "allocated reliability" more or less well defined and hence insensitive to the preference assessment that will rank the solutions (A6, B5, C8, D8). For example, Table 3.5 suggests very well defined performance criteria for the Feedwater/Power Conversion Systems [X(6)] and its recovery for containment heat removal purposes [X(19)], as well as, for the High Pressure Injection Systems [X(8), X(9)] and the recovery of the support systems [X(13)]. A somewhat wider range is suggested for the SLCS, the FWPCSL, and the Low Pressure Injection Systems. Systems belonging to the third category, however, cannot be characterized by a well defined "performance criterion" or "allocated reliability" before further preference assessment.

Let us suppose that after a second phase of preference assessment, solutions A6 and D8 are eliminated in favor of B5 and C8, respectively. This elimination results in the ranges of the system unreliabilities given in Table 3.6. There is no wide range category in this new tabulation since the space of "optimum" solutions has been decreased substantially. Now, only five systems [(X(1), X(4), X(14), X(15), X(16)] have a range wide enough that require elimination of one of the two remaining noninferior solutions. If for example, the two solutions (B5) and (C8) are considered almost equivalent, that is, if the increase in the cost from B5 to C8 is of equal value to the corresponding decrease in the other attributes, then any plant design with

*This would not necessarily be the case for all reactor designs and sites.

system unreliabilities in the ranges given in Table 3.6 would be acceptable, in the sense that we expect that a plant specific PRA model would demonstrate outcomes (C_d, A, L, G) near the optimum range. Comparing the "aspiration" values of Table 3.6 with the assessed values of the model plant design (Table 3.2) we observe the following. Subject to the validity of the assumed cost functions (see Section B.2 and Table B.4 in Appendix B for the particular cost functions used) and the PRA model used (see cautionary statement at the beginning of Section 3), there is room for improvement in the unreliabilities of the model plant. Improvement here means that the present design of the model plant represents an inferior solution since it could be possible to improve the scores in the evaluation indices (C_d, A, L, G) by changing the unreliabilities of the safety systems. In particular, we observe (see Tables 3.2 and 3.6) that the "optimal" solution suggests lower values for the Feedwater/Power Conversion System unreliabilities both for early and late decay heat removal functions [variables X(6) and X(15)] as well as a lower failure probability to recover the late decay heat removal function [variable X(19)]. The optimal solution also suggests lower unreliabilities for the High Pressure Injection Systems [variables X(8) and X(9)] and for the containment heat removal function RHRH lower unreliability for the Standby Liquid Control System [X(2)] and a higher unreliability for the Reactor Protection System [X(1)]. Higher unreliability values are suggested for the Low Pressure Injection Systems [X(11) and X(12)], the Service Water System [X(5)], and the hardware for the Automatic Depressurization System [X(10)]. Finally, the model plant unreliability values for the DC power supply [X(4)], the diesel generators [X(16)], and the failure probability for manual initiation of the depressurization system are near the calculated "optimal" values.

Table 3.7 shows the safety function unreliabilities corresponding to the four noninferior solutions (A6, B5, C8, D8) in comparison to the model plant nominal values. The results for the function level unreliabilities are similar to those for the system and component level unreliabilities. In particular, we observe from Table 3.7 that compared to the model plant nominal values the "optimum" solution suggests lower unreliabilities for the feedwater injection function [Q] and the high pressure injection function [U]. It also suggests a lower unreliability for the poison injection function [C'] served by the Standby Liquid Control System. However, higher unreliabilities are suggested for the low pressure injection function [V], and for the reactor subcriticality function [C] served by the Reactor Protection System. All these observations are, of course, subject to the validity of the assumed cost functions.

Another observation from Table 3.7 is that the value of the expected acute fatalities is very small for the model plant nominal case and outside the range of the noninferior solutions. The same is true, although in the opposite (too high) direction, for the cost.

The top level attributes for the four noninferior solutions and the model plant nominal case are displayed in Figure 3.3 and compared to a set of proposed safety goals.

3.2 Comparison with Other Approaches

The proposed approach has significant advantages over other evaluation approaches such as performing a PRA and "inspecting" the results along with some form of cost/benefit analysis.

The results of PRA provide a single, static image of the plant in the consequence space. That is, given the PRA model its quantification at a specific level of unreliability values provides the corresponding levels of the consequences (safety objectives-attributes). An importance analysis can then provide the relative values of particular changes of individual components and suggest the direction of maximum benefit that could be achieved by a change of the unreliability of a single component. The evaluation (in the consequence space) of a specific alternative consisting of the changes of more than one component unreliability requires the requantification of the PRA model. On the other hand, the proposed methodology provides as its solution the noninferior subspace in the decision space. Any alternative (proposed change in the design or backfitting) can be directly evaluated by examining whether or not it belongs to the noninferior set. If it does, it is initially "acceptable" and further comparison with other "noninferior" solutions requires a preference assessment. If it does not, then this alternative should not be acceptable since there is at least another alternative that can achieve the same level of health consequences at a lower cost or lower level of health consequences at the same cost.

In addition, given a specific point in the decision space (specific design or operating plant) and the noninferior subspace, one can identify the necessary changes in the component unreliabilities that will bring the plant into the noninferior subspace.

Let us consider, for example, the case of the nominal Limerick plant as an initial design of a new plant. The unreliabilities of the components (point $\underline{x}$ in the feasible space) are given in Table 3.2. The corresponding values of the four attributes (point $\underline{z}$ on the outcome space) are given in Table 3.7. Let us further suppose that it is desired to alter this design in the most cost-effective way so that the frequency of core damage becomes 5×10^{-5}/ryear, keeping the acute fatalities at the same level.

Given the results of the analysis of the base model (Section 3.3) it is immediately evident that the objective is to bring the design to a part of the noninferior set that is characterized by a frequency of core damage equal to 5×10^{-5}/ryear. The trace of this part of the noninferior set in the outcome space is given in Figure 3.1 and in tabular form in Table 3.8. This table also gives the corresponding section of the noninferior set in the decision space. Perusal of this table indicates that the wanted end result is a point between points D2 and D3 and closer to point D3 ($C_d = 5\times10^{-5}$, $A = 5\times10^{-5}$ compared to the desired $C_d = 5\times10^{-5}$, $A = 4.57\times10^{-5}$). Comparison of point $\underline{x}$ of the initial design (also given in Table 3.8) with point $\underline{x}_3$ immediately provides the necessary changes in the component unreliabilities that must be made. These changes are shown in the last column of Table 3.8.

To reach the same results with successive importance and cost/benefit analyses[24] is, for all practical purposes, impossible.

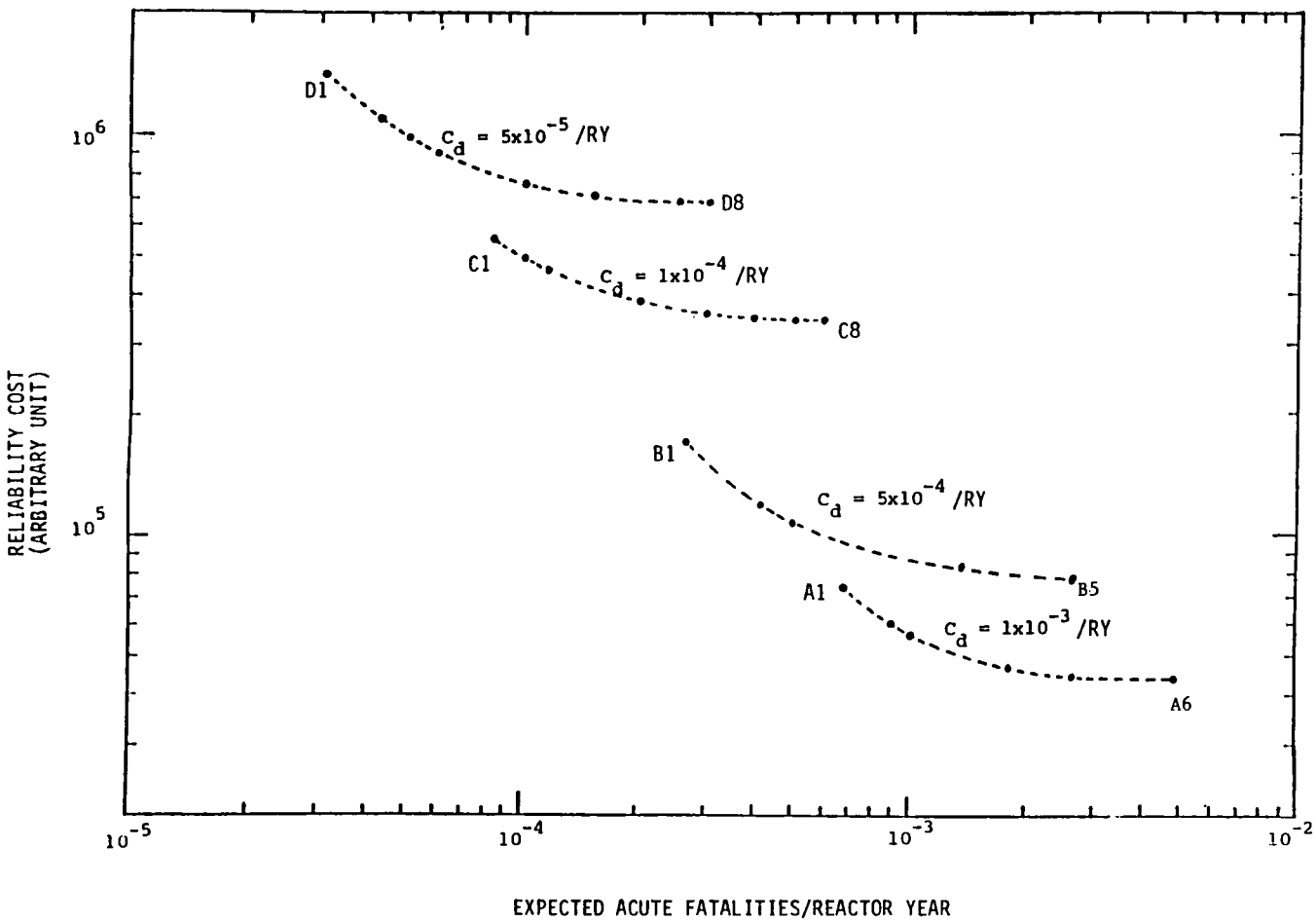


Figure 3.1 A two-dimensional display of noninferior outcomes at several core damage frequencies for the base model.

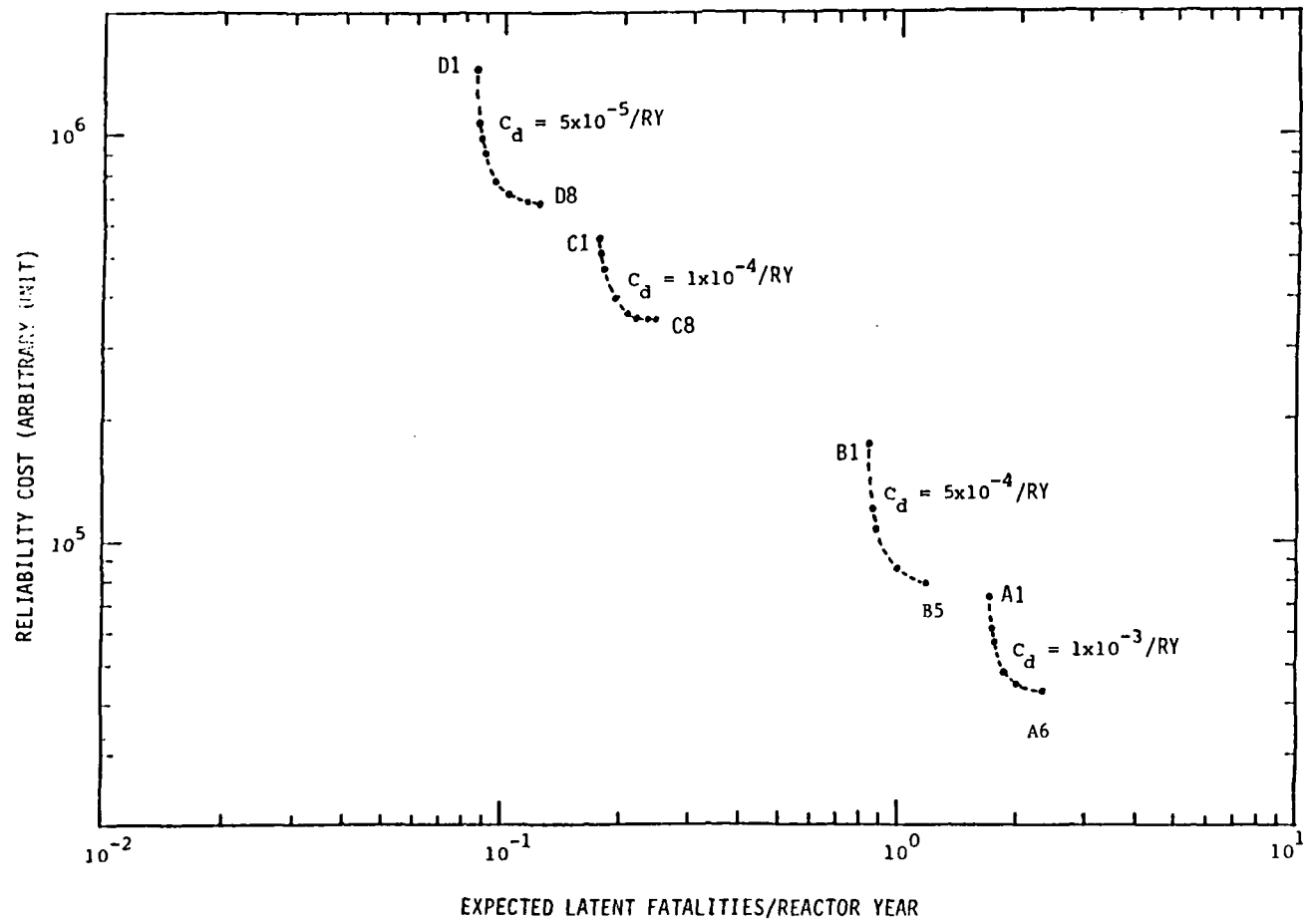


Figure 3.2 A two-dimensional display of noninferior outcomes at several core damage frequencies for the base model.

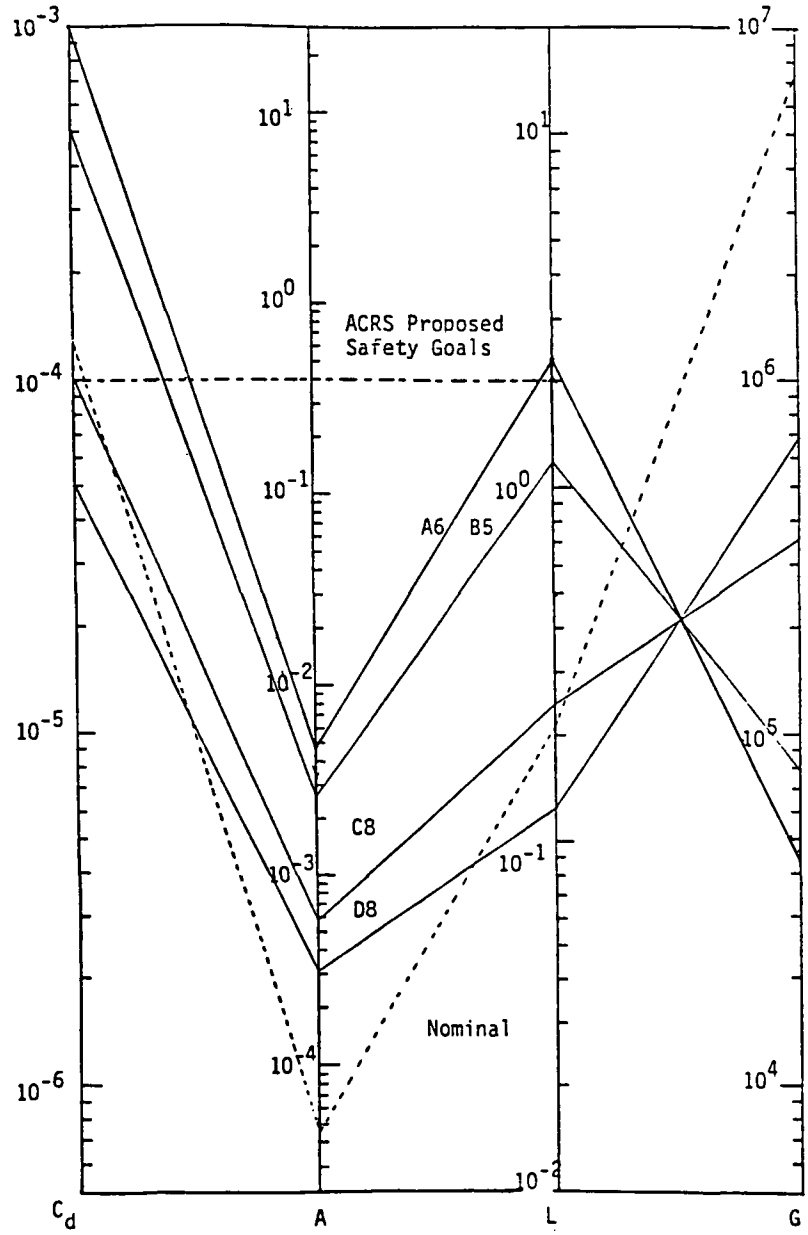


Figure 3.3 Attribute profiles of noninferior outcomes for the base model in comparison with ACRS proposed safety goals and model plant nominal values.

Table 3.1 List of "Decision Variables"

X(I)	Name	Event Description
1	RPS(M)	Mechanical failure of reactor protection system
2	SLCSH	Hardware failure of standby liquid control system
3	LOSP	Transient induced loss of offsite power
4	EDC	Loss of all DC (loss of all AC for more than four hours or other failures in DC power supply system)
5	WSW	Loss of service water
6	FWPCS	Hardware failure of the feedwater and PCS system
7	ARC	Operator failure to provide alternate room cooling to frontline system rooms
8	RCICH	Hardware failure of reactor core isolation cooling system
9	HPCIH	Hardware failure of high pressure coolant injection system
10	ADSH	Hardware failure of automatic depressurization system
11	LPCIH	Hardware failure of low pressure coolant injection system
12	LPCSH	Hardware failure of low pressure core spray system
13	RECOV	Failure to recover the support system
14	RHRH	Hardware failure of residual heat removal system
15	FWPCSL	Hardware failure of feedwater and PCS system for long-term containment heat removal
16	DG	Failure of diesel generator system
17	X	Operator failure to actuate the ADS
18	D	Operator failure to inhibit ADS actuation in ATWS events
19	FWPCSL(RECOV)	Failure to recover feedwater and PCS hardware in 20 hours given that it failed in early phase (Q)

Table 3.2 Input Range of Component Unreliabilities

X(I)	Name	Model Plant Nominal Mean Unavailability	Lower Limit	Upper Limit
1	RPS(M)	1.0(-5)	1.0(-7)	1.0
2	SLCSH	3.5(-3)	1.0(-4)	1.0
3	LOSP	5.2(-4)	5.2(-4)(Fixed)	5.2(-4)
4	EDC	2.5(-7)	1.0(-7)	1.0
5	WSW	5.0(-7)	1.0(-7)	1.0
6	FWPCS	2.0(-2)	5.0(-3)	1.0
7	ARC	1.5(-1)	1.5(-1)(Fixed)	1.5(-1)
8	RCICH	7.0(-2)	1.0(-2)	1.0
9	HPCIH	1.16(-1)	1.0(-2)	1.0
10	ADSH	1.76(-4)	1.0(-5)	1.0
11	LPCIH	1.8(-3)	1.0(-4)	1.0
12	LPCSH	2.6(-3)	1.0(-4)	1.0
13	RECOV	1.7(-1)	5.0(-2)	1.0
14	RHRH	4.5(-5)	1.0(-5)	1.0
15	FWPCSL	6.0(-2)	1.0(-3)	1.0
16	DG	9.7(-4)	1.0(-4)	1.0
17	X	6.0(-3)	1.0(-10)*	1.0
18	D	2.0(-3)	2.0(-3)(Fixed)	2.0(-3)
19	FWPCSL(RECOV)	3.6(-1)	5.0(-2)	1.0

*The design of the plant provides for an automatic initiation of depressurization for LOCA initiators. Transient initiators, however, require manual initiation. A low value of X means that the need for manual initiation has been removed and that automatic initiation is provided for transient initiators.

Table 3.3 Noninferior Solutions with Least Cost from Each Group (See Figure 3.1)

	A6	B5	C8	D8
C_d	1.00(-3)	5.00(-4)	1.00(-4)	5.00(-5)
A	4.93(-3)	2.66(-3)	5.87(-4)	3.01(-4)
L	2.32(0)	1.19(0)	2.47(-1)	1.24(-1)
G	4.37(+4)	7.95(+4)	3.52(+5)	6.87(+5)
X(1)	3.04(-3)	1.65(-3)	3.66(-4)	1.88(-4)
X(2)	1.05(-3)	7.27(-4)	3.15(-4)	2.21(-4)
X(3)	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)
X(4)	5.33(-5)	2.73(-5)	5.57(-6)	2.80(-6)
X(5)	1.19(-4)	6.10(-5)	1.25(-5)	6.26(-6)
X(6)	8.32(-3)	5.31(-3)	5.00(-3)	5.00(-3)
X(7)	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)
X(8)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	1.36(-2)	6.79(-3)	1.43(-3)	7.20(-4)
X(11)	5.79(-2)	3.75(-2)	1.31(-2)	7.99(-3)
X(12)	5.62(-2)	3.56(-2)	1.23(-2)	8.09(-3)
X(13)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	3.20(-3)	2.05(-3)	5.40(-4)	2.89(-4)
X(15)	5.51(-3)	3.52(-3)	1.40(-3)	1.00(-3)
X(16)	3.22(-3)	1.65(-3)	3.36(-4)	1.69(-4)
X(17)	1.36(-2)	7.44(-3)	1.43(-3)	7.20(-4)
X(18)	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)
X(19)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)

Table 3.4 Aspirations after Preliminary Screening for the Base Model

X(i)	Name	X_L	X_U
1	RPS(M)	1.88(-4)	3.04(-3)
2	SLCSH	2.21(-4)	1.05(-3)
4	EDC	2.80(-6)	5.33(-5)
5	WSW	6.26(-6)	1.19(-4)
6	FWPCS	5.00(-3)	8.32(-3)
8	RCICH	1.00(-2)	1.00(-2)
9	HPCIH	1.00(-2)	1.00(-2)
10	ADSH	7.20(-4)	1.36(-2)
11	LPCIH	7.99(-3)	5.79(-2)
12	LPCSH	8.09(-3)	5.62(-2)
13	RECOV	5.00(-2)	5.00(-2)
14	RHRH	2.89(-4)	3.20(-3)
15	FWPCSL	1.00(-3)	5.51(-3)
16	DG	1.69(-4)	3.22(-3)
17	X	7.20(-4)	1.36(-2)
19	FWPCSL(RECOV)	5.00(-2)	5.00(-2)

Table 3.5 Groupings of Aspirations after First Step of Preference Assessment for the Base Model

I. VERY NARROW RANGE ($X_U \leq 2X_L$)

	Name	Unavailability Range
X(6)	FWPCS	5.00(-3) - 8.32(-3)
X(8)	RCICH	1.00(-2) - 1.00(-2)
X(9)	HPCIH	1.00(-2) - 1.00(-2)
X(13)	RECOV	5.00(-2) - 5.00(-2)
X(19)	FWPCSL(RECOV)	5.00(-2) - 5.00(-2)

II. NARROW RANGE ($2X_L < X_U \leq 10X_L$)

	Name	Unavailability Range
X(2)	SLCSH	2.21(-4) - 10.5(-4)
X(11)	LPCIH	7.99(-3) - 57.9(-3)
X(12)	LPCSH	8.02(-3) - 56.2(-3)
X(15)	FWPCSL	1.00(-3) - 5.51(-3)

III. WIDE RANGE ($10X_L < X_U$)

	Name	Unavailability Range
X(1)	RPS(M)	1.88(-4) - 30.4(-4)
X(4)	EDC	2.80(-6) - 53.3(-6)
X(5)	WSW	6.26(-6) - 119.(-6)
X(10)	ADSH	7.20(-4) - 136.(-4)
X(14)	RHRH	2.89(-4) - 32.0(-4)
X(16)	DG	1.69(-4) - 32.2(-4)
X(17)	X	7.20(-4) - 136.(-4)

Table 3.6 Groupings of Aspirations after Second Step of Preference Assessment for the Base Model

I. VERY NARROW RANGE ($X_U \leq 2X_L$)

X(6)	FWPCS	5.00(-3) - 5.31(-3)
X(8)	RCICH	1.00(-2) - 1.00(-2)
X(9)	HPCIH	1.00(-2) - 1.00(-2)
X(13)	RECOV	5.00(-2) - 5.00(-2)
X(19)	FWPCSL(RECOV)	5.00(-2) - 5.00(-2)

II. NARROW RANGE ($2X_L < X_U \leq 10X_L$)

X(1)	RPS(M)	3.66(-4) - 16.5(-4)
X(2)	SLCSH	3.15(-4) - 7.27(-4)
X(4)	EDC	5.57(-6) - 27.3(-6)
X(5)	WSW	1.25(-5) - 6.10(-5)
X(10)	ADSH	1.43(-3) - 6.79(-3)
X(11)	LPCIH	1.31(-2) - 3.75(-2)
X(12)	LPCSH	1.23(-2) - 3.56(-2)
X(14)	RHRH	5.40(-4) - 20.5(-4)
X(15)	FWPCSL	1.40(-3) - 35.2(-3)
X(16)	DG	3.36(-4) - 16.5(-4)
X(17)	X	1.43(-3) - 7.44(-3)

Table 3.7 Function* Unavailabilities Corresponding to Noninferior Solutions with Least Cost from Each Group and Model Plant Nominal Unreliabilities

	A6	B5	C8	D8	Model Plant Nominal
C_d	1.00(-3)	5.00(-4)	1.00(-4)	5.00(-5)	1.26(-4)**
A	4.93(-3)	2.66(-3)	5.87(-4)	3.01(-4)	4.57(-5)
L	2.32(0)	1.19(0)	2.47(-1)	1.24(-1)	2.12(-1)
G	4.37(+4)	7.95(+4)	3.52(+5)	6.87(+5)	7.24(+6)***
C	3.04(-3)	1.65(-3)	3.66(-4)	1.88(-4)	1.00(-5)
C'	1.10(-3)	7.55(-4)	3.21(-4)	2.24(-4)	3.50(-3)
Q	9.01(-3)	5.92(-3)	5.54(-3)	5.53(-3)	2.05(-2)
U	1.71(-4)	1.37(-4)	1.07(-4)	1.04(-4)	8.12(-3)
V	1.70(-2)	8.21(-3)	1.61(-3)	7.94(-4)	1.82(-4)
W	2.63(-5)	1.16(-5)	1.66(-6)	7.41(-7)	2.83(-6)

*Functions are defined in Table B.2.

**This value reflects the fact that the PRA model used in this study does not include recovery of loss of offsite power.

***This value was derived by substituting the model plant nominal mean unavailabilities shown in Table B.5 into the cost functions in Section B.2 with parameters in Table B.4. Recall that the same cost functions and associated parameters were used to generate the noninferior solutions (A6, B5, C8, D8).

Table 3.8 Noninferior Solutions at Core Damage Frequency 5.0(-5) for the Base Model and Model Plant Nominal Values

	D1	D2	D3	D8	Model Plant Nominal	*
C_d	5.00(-5)	5.00(-5)	5.00(-5)	5.00(-5)	1.26(-4)	
A	3.01(-5)	4.17(-5)	5.00(-5)	3.01(-4)	4.57(-5)	
L	8.64(-2)	8.78(-2)	8.90(-2)	1.24(-1)	2.12(-1)	
G	1.43(+6)	1.10(+6)	9.93(+5)	6.87(+5)	7.24(+6)	
X(1)	1.19(-5)	1.93(-5)	2.47(-5)	1.88(-4)	1.00(-5)	+
X(2)	9.90(-4)	7.54(-4)	6.61(-4)	2.21(-4)	3.50(-3)	-
X(3)	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)	0
X(4)	3.15(-6)	3.07(-6)	3.04(-6)	2.80(-6)	2.50(-7)	+
X(5)	6.35(-6)	6.59(-6)	6.63(-6)	6.26(-6)	5.00(-7)	+
X(6)	5.00(-3)	5.00(-3)	5.00(-3)	5.00(-3)	2.00(-2)	-
X(7)	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)	0
X(8)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	7.00(-2)	-
X(9)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.16(-1)	-
X(10)	8.11(-4)	7.90(-4)	7.82(-4)	7.20(-4)	1.76(-4)	+
X(11)	8.18(-3)	8.45(-3)	8.44(-3)	7.99(-3)	1.80(-3)	+
X(12)	8.28(-3)	8.53(-3)	8.53(-3)	8.09(-3)	2.60(-3)	+
X(13)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	1.70(-1)	-
X(14)	2.35(-4)	2.75(-4)	2.87(-4)	2.89(-4)	4.50(-5)	+
X(15)	1.00(-3)	1.00(-3)	1.00(-3)	1.00(-3)	6.00(-2)	-
X(16)	1.90(-4)	1.85(-4)	1.83(-4)	1.69(-4)	9.70(-4)	-
X(17)	8.11(-4)	7.90(-4)	7.82(-4)	7.20(-4)	6.00(-3)	-
X(18)	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)	0
X(19)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	3.60(-1)	-

*Necessary changes in unavailabilities to bring the initial design to the desired one (+: ought to increase, -: ought to decrease).

4. CONCLUSIONS, LIMITATIONS, AND RECOMMENDATIONS

4.1 Conclusions

The allocation methodology we developed was based on a PRA model, reliability cost functions, and a set of multiple flexible top level criteria. The particular aspects of the methodology, i.e., (1) the multiobjective programming approach (the decoupling of the preference assessment from the technical analysis), and (2) the treatment of the top level criteria as flexible criteria, provide a full exposition of the problem and suggest useful options to the decision maker: plant designer, plant owner, or regulator as appropriate.

More specifically, the experience with an application of the methodology to a nontrivial example that contains most of the aspects of a complete PRA model (including containment performance as the decision variables and a seismic sequence) demonstrates that the methodology is operational. The methodology provides valuable information to the decision maker in the sense that it offers the various viable (noninferior) options (and only the viable options), for the set of top level criteria and their self-consistently associated plant specific performance characteristics and thus renders the viable solutions more amenable to a preference assessment. Therefore, the dimension and difficulty of the decision problem of allocating reliabilities can be reduced substantially even without a formal preference assessment. The results of the example problem also indicate that many of the allocated reliabilities are insensitive to a range of choices of top level criteria while only a few reliabilities are sensitive.

It is recognized, however, that a complete preference assessment is a necessary step to an ultimate resolution of a decision problem, i.e., choosing a single allocation from the noninferior solution set. A potentially useful approach to this seems to be the decomposition method discussed in Appendix C.

A brief study of how to incorporate the uncertainty in the allocation procedure indicates that a "formal" uncertainty analysis (formal in the sense of considering uncertainties before solving the allocation problem) is feasible and computationally affordable under a set of special assumptions. This is the α-confidence level approach described in Appendix D. In a more general but less formal approach, however, we can employ several uncertainty propagation techniques to assess the variation of global attributes due to uncertainties of the various variables in the models, once we solve the allocation problem using point (e.g., mean) values.

The design differences in the various existing nuclear power plants render a generic allocation difficult. The dependency due to commonalities of the front line systems and the support systems makes an allocation at a functional level infeasible on a generic basis. Standardized light water reactors or advanced reactors in the design stage would, however, be much more amenable to a generic allocation.

While information on the reliability cost functions was identified as a necessary ingredient in the allocation scheme, the detailed and realistic specification of cost functions seems to be a difficult task. The meaningfulness of the allocation relies also on the veracity of the chosen risk model. If the risk model is based on unrealistic assumptions or is significantly

incomplete, the usefulness of the allocation as criteria will be diminished. However, in spite of these limitations (see also the following section), the process of the methodology application will serve in most of the situations as valuable guidance to reliability design and improvement of nuclear reactor systems, which could be used to supplement more traditional methods. In particular, the proposed methodology provides more and better information about the characteristics, the safety importance and the cost-effective modifications of a given plant design than simpler approaches such as inspection of PRA results coupled with importance/sensitivity analysis. A PRA provides a "static" image of the plant corresponding to a particular level of the constituent unreliabilities. An importance analysis provides information on the effect of changes of individual components. Any other modification of the design involving unreliability changes of more than one component must be evaluated separately. The developed methodology, however, starting with all feasible alternatives of component unreliabilities and system configurations, examines and evaluates all possible combinations in a systematic and efficient way.

In conclusion, the following have been accomplished in view of the stated objectives of the study:

(1) The technical feasibility of the development of a set of self consistent reliability criteria for plant systems, major components and operational practices has been demonstrated for a given plant configuration.

(2) The development of a generic set of low-level reliability criteria is not feasible with the developed methodology since it would require a corresponding generic plant configuration. There is no such generic configuration that can cover the wide design spectrum of the presently operating LWRs.

(3) The methodology has been applied to a realistic complex problem.

(4) The achievability of the developed criteria is guaranteed by definition since the developed approach is a "forward" approach, i.e., one that starts from all the feasible allocations and determines the viable alternatives.

(5) A number of problems and limitations have been identified and presented in Section 4.2.

4.2 Limitations

4.2.1 PRA Models

The current PRA models provide the most comprehensive descriptions of safety aspects of nuclear power plants. Although it is recognized that the PRA models have limitations and weaknesses,[28,29] it is believed that, as the state-of-the-art in PRA models and methodology improves, the usefulness of the reliability allocation for criteria development will increase. It is interesting to note that the process and the results of a sensitivity study (see Appendix B) with the allocation methodology shed lights on the PRA models themselves (e.g., the effects of uncertainties in the site matrix) and provide

valuable information to the person who faces a decision making problem under uncertainty.

4.2.2 Approximations in Computational Models

The PRA model of a plant provides only a computationally tractable set of dominant accident sequences represented by minimal cut sets. These dominant sequences and cut sets are obtained after truncation processes operating on the accident sequences which consist of all possible combinations of events. These truncation processes are based on the "nominal" probabilities of the events in the sequences and on a predefined cutoff criterion. Thus, the proposed methodology operating on the dominant sequences does not take into consideration the "residual" risks that may be attributed to the truncated sequences and cut sets. More accurate treatments will require more sequences and cut sets and thus greater computational times.

A more precise representation of a PRA accident sequence requires NOT events in the minimal cut sets (prime implicants). Given a minimal cut set expression of a sequence, calculational approximations better than the usual rare event approximation would also be desirable for improved accuracy. Non-convexity introduced by NOT events and/or by better-than-rare event approximations no longer guarantees global optimality of the noninferior solutions and only assures local optimality. Although there exist several techniques designed for global solutions in these situations, they are algorithmically less well-established than the techniques for local solutions and invariably they require much more computational effort. It is not clear at this time whether the more sophisticated techniques for global solutions are worth the effort in our problem. The rare event approximation is, however, a conservative one and is usually very accurate except for some pathological cases. Appendix A contains an analysis of the rare event approximation in the context of reliability allocation for a simple model system.

4.2.3 Reliability Cost Functions

The functional forms and associated parameters of reliability cost functions used in this study were chosen for illustration purposes. However, they portray, qualitatively, the correct trends which realistic cost functions would exhibit. The detailed reliability cost functions are to be specified by field data. Although this may not be an easy task, an increased effort in this area is warranted in view of not only its importance in reliability allocation but also its potential usefulness in other contexts of decision making.

4.3 Recommendations

The following is a list of recommendations for future directions of the program, not necessarily in order of importance and priority:

i) Application of the methodology to different designs to assess the extent of "generic" allocation. Investigation of possible "groupings" of power plant designs.

ii) Application of the methodology to a more realistic problem, i.e., a) a full PRA model, including more accurate representations, e.g., NOT events, other common cause failures, other external events,

b) several alternatives in configurations of a plant (see Section 2.3), c) realistic cost models.

iii) Exploration of approaches to preference assessment, e.g., the decomposition method discussed in Appendix C. Examination of the validity of the additive independence assumption and the use of certainty equivalents (see Appendix C).

iv) Investigation of the usefulness of the reliability allocation as a means of monitoring and verifying a plant's performance and of assessing compliance with a set of general objectives on a plant-specific basis.

v) Uncertainty analysis along the lines of one or more approaches identified in Appendix D, or of some other approaches.

vi) Extension of the methodology to treat not only safety aspects but also operational aspects, e.g., availability, of the nuclear power plants.

vii) Application of the methodology to the development of particular performance criteria, e.g., development of containment performance criteria.

viii) Refinement of the methodology through interactions with PRA practitioners and decision makers (plant designers, plant owners, or regulators as appropriate).

REFERENCES FOR MAIN REPORT

1. U.S. Nuclear Regulatory Commission, "An Approach to Quantitative Safety Goals for Nuclear Power Plants", NUREG-0739, October 1980.

2. U.S. Nuclear Regulatory Commission, "Safety Goals for Nuclear Power Plants: A Discussion Paper", NUREG-0880, February 1980.

3. U.S. Nuclear Regulatory Commission, "Safety Goals for Nuclear Power Plant Operation", NUREG-0880, Revision 1, May 1983.

4. Atomic Industrial Forum, "A Proposed Approach to the Establishment and Use of Quantitative Safety Goals in the Nuclear Regulatory Process", The Atomic Industrial Forum Committee on Reactor Licensing and Safety, May 1981.

5. Joksimovich, V., O'Donnell, L. F., "Quantitative Goals for the Regulatory Process", GA-A16119, October 1980.

6. Starr, C., "Risk Criteria for Nuclear Power Plants: A Pragmatic Proposal", ANS/ENS International Conference, Washington, D.C., November 1980.

7. Okrent, D., Apostolakis, G., Whitley, R., Garrick, B. J., "On PRA Quality and Use", Chapter 4, UCLA-ENG-8269, October 1982.

8. Ebersole, J. C., "ACRS Comments on Task Action Plan A-45, Shutdown Decay Heat Removal Requirements", Advisory Committee on Reactor Safeguards Letter to W. J. Dirks, dated August 14, 1984.

9. Sauter, G. D., Hughes, E. A., "The Applicability of Quantitative Safety Goals in the NRC's Regulatory Process", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, February, 1985, San Francisco, California.

10. Thadani, A. C., "SRP 10.4.9, Auxiliary Feedwater System (PWR)", NRC Internal Memorandum, June 1981.

11. U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", NUREG-75/014 (WASH-1400), October 1975.

12. U.S. Nuclear Regulatory Commission, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse Designed Operating Plants", NUREG-0611, January 1980.

13. Cave, L., Kastenberg, W. E., "Development of Quantitative Screening Criteria for the Decay Heat Removal Systems of Light Water Reactors Volume 1 Pressurized Water Reactors", Sandia National Laboratories, Draft, May 1983.

14. Knoll, A., "Component Cost and Reliability Importance for Complex System Optimization", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Volume II, Port Chester, NY, September 1981.

15. Burdick, G. R., Rasmuson, D. M., Weisman, J., "Probabilistic Approaches to Advanced Reactor Design Optimization", in Nuclear System Reliability Engineering and Risk Assessment, Edited by Fussell and Burdick, SIAM, Philadelphia, PA, 1977.

16. Hartung, J., "LMFBR Safety Criteria: Cost-Benefit Considerations Under the Constraint of an A Priori Risk Criterion", Proceedings of the International Meeting on Fast Reactor Safety Technology, Volume III, Seattle, WA, August 1979.

17. Gokcek, O., Temme, M. I., Derby, S. L., "Risk Allocation Approach to Reactor Safety Design and Evaluation", Proceedings of the Topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety, Volume 2, Los Angeles, CA, May 1978.

18. Hurd, D. E., "Risk Analysis Methods Development April-June 1980", General Electric, GEFR-14023-13, July 1980.

19. Fischhoff, B., "Standard Setting Standards: A Systematic Approach to Managing Public Health and Safety Risks", Decision Research, NUREG/CR-3508, February, 1984.

20. Cohon, J. L., Multiobjective Programming and Planning, Academic Press, New York, 1978.

21. Goicoechea, A., Hansen, D. R., Duckstein, L., Multiobjective Decision Analysis with Engineering and Business Applications, John Wiley and Sons, New York, 1982.

22. Rowe, M. D., Hobbs, B. F., Pierce, B. L., Meier, P. M., "An Assessment of Nuclear Power Plant Siting Methods", Brookhaven National Laboratory, NUREG/CR-1689, July 1981.

23. Keeney, R., Raiffa, H., Decisions with Multiple Objectives: Preferences and Value Tradeoffs, Wiley, New York, 1976.

24. Garrick, B. J., "Examining the Realities of Risk Management", Presented at the Society for Risk Analysis 1984 Annual Meeting, Knoxville, TN, September 30 - October 3, 1984.

25. Boyd, D. W., "A Methodology for Analyzing Decision Problems Involving Complex Preference Assessments", Ph.D. Dissertation, Stanford University, May 1970.

26. Papazoglou, I. A., et al., "A Review of the Limerick Generating Station Probabilistic Risk Assessment", Brookhaven National Laboratory, NUREG/CR-3028, February 1983.

27. Philadelphia Electric Company, "Probabilistic Risk Assessment Limerick Generating Station", Docket Nos. 50-352, 353, June 1982.

28. Joksimovich, V., et al., "A Review of Some Early Large Scale PRA Studies", NUS Corporation, EPRI NP-3265, October 1983.

29. U.S. Nuclear Regulatory Commission, "Probabilistic Risk Assessment (PRA) Reference Document", NUREG-1050, September 1984.

PART II

TECHNICAL APPENDICES

APPENDIX A

METHODOLOGY DETAILS

A.1 Allocation of Top Level Safety Criteria

The general objective of the study is to examine the feasibility of the allocation (decomposition) of a set of top level safety criteria to system reliability and containment performance requirements. Such a decomposition would provide a "performance criteria" set in successive tiers of increasing specificity, that could constitute a workable risk management framework for LWRs which is compatible with the needs of reactor designers and operators and is consistent with the top level quantitative safety criteria.[1] NRC's proposed safety goals and numerical guidelines[2] would provide an example of such top level safety criteria. Three questions are then raised in relation to this general objective:

1) Is the definition of a set of safety criteria meaningful?

2) Is it useful (necessary) to decompose the safety criteria into system performance criteria?

3) Is it possible (feasible) to decompose the safety criteria into system performance criteria on a generic basis?

From a very narrow technical point of view one could argue that questions 1 and 2 are irrelevant to our problem and that the study has as its objective to provide a detailed answer to the third question conditional on the existence of meaningful safety criteria. Very early in our study, however, it became apparent that Question #3 could not be addressed in complete isolation of the first two and the comments of the Steering Group supported this conclusion.* It was established, for one, that a rational and meaningful decomposition of a proposed set of safety criteria (i.e., core damage frequency, expected acute fatalities and latent fatalities) was not possible unless cost considerations were introduced into the picture. Thus, we will assume that a set of multiple global (top level) risk indices** (along with a cost measure) is defined. It was also established that, since different levels of safety criteria are attainable at different costs, a solution to the problem will not be complete without a preference assessment (value tradeoffs)*** among the various global risk indices. These two points bear to the fundamental question of whether "standard setting" constitutes a better way of regulation than "case-by-case decision making." Decision making procedures attempt to order options according to relative attractiveness; standards simply categorize them as "acceptable/not acceptable".[3] The present state of regulation is a mixture of these two ways of regulation in that it employs a case-by-case review on alternatives (plants) that have been already designed and built according

*This conclusion is further supported by our informal discussions with several members of the nuclear industry/community.

**We use the word "indices" when referring to attributes without numerical values while the word "criteria" accompanies numerical values.

***The cost-benefit guideline of $1000 per person-rem in Ref. 2 is a value tradeoff.

to a set of design standards. In this study we do not attempt to resolve this issue but we do take the technical position that the set of global risk indices whether used as a basis for developing standards or used as "performance indices" for decision making purposes should include cost considerations. Furthermore, we claim that a preference assessment on the various safety and cost measures is a necessary step for a meaningful regulatory procedure based on either approach. This latter issue is, however, a basic policy question and in this study we simply suggest a procedure (in Appendix C) for addressing it.

Having partially resolved the first question in that we agreed on a set of multiple global risk indices (along with a cost measure), we can now concentrate on the last two. Question #2 is very important itself and relevant to the third question because the answer to the usefulness question is a preempting condition to the feasibility question. This point was particularly stressed by one of the members of the Steering Group.

The answer to question #2 is a difficult one. It relates to the potential for implementing a set of proposed safety criteria and to the regulatory process in general. We will only offer a few thoughts. One could argue that performance indices at a system level are not useful or necessary and even further that they would constitute overregulation. The argument would go that once the safety criteria (including cost considerations and trade-offs) are established, what would matter is whether a particular plant satisfies the criteria or not. How to satisfy the criteria is not a regulatory function. A counterargument could be, however, that even the proposed safety criteria constitute a decomposition of a more general and lofty goal which could be stated as "Produce electricity from nuclear power plants reliably, economically, and safely." The question then reduces to: "At what level do the decomposition and, consequently, the specific regulatory guidance stop?" Another consideration could be that from a viewpoint of experiential data, it is more difficult to "monitor" and "verify" the higher level of safety criteria, e.g., core damage frequency and expected acute and latent fatalities, than the lower level of safety criteria, e.g., system or component reliabilities.

This is equivalent to asking whether the regulatory process should concentrate on the technical details or on the overall performance of the technology. Although the question is of great policy importance, we see as part of our objectives to answer this question from a technical point of view. That is, to suggest the level at which it is possible to decompose a regulatory policy set on the performance of the technology (safety/overall cost) to a regulatory policy on the technical aspects (system performance requirements) and to do that in a self consistent way so that "compliance" at the technical level would imply "compliance" at the overall performance level. It is noteworthy that presently there exists a rather detailed fabric of regulations on the technical aspects of the nuclear technology. There exist specific requirements that actually determine the basic composition of the nuclear power plants as a system--at least from a safety point of view. Thus, specific systems such as the Reactor Protection System and the various decay heat removal systems are dictated by regulation. There are also some deterministic requirements that prescribe several of the characteristics of these systems; e.g., the "single failure criterion." Suppose that the regulator considers the introduction of a regulatory requirement that would require Auxiliary Feedwater Systems (AFWS) in PWRs to have three pumps. This requirement would

constrain the design of PWRs in two ways. First, it requires an AFWS and second it requires a three-pump system. Such ad-hoc system performance requirements may or may not lead to lower levels of risk than those intended by the standard setter (regulatory policy on the technology performance). The replacement/extension, on the other hand, of such ad-hoc standards at the system level by standards developed by a systematic and consistent decomposition of general safety/cost objectives would result in a regulation of the technical nspects of the technology that is consistent with its performance requirements. In addition, it could present additional guidance to the reactor designers and operators on how to satisfy the global safety criteria. In general, however, the finer the level of the decomposition the more rigid the regulation and the more the burden of safe design and operation is shifted from the plant owner and operator to the regulatory agency.

As far as the third question is concerned, given the present state of understanding of the problem, the authors believe that a decomposition of a set of safety criteria into reliability performance requirements at great levels of specificity is not possible on a generic basis. This is due to the design differences that characterize the various nuclear power plants; these differences are exhibited as dependences of the frontline* systems on the support* systems. It would be interesting, however, to examine in future work the possibility of distinguishing between a number of classes of designs (e.g., BWRs, 2-3-4 loop Westinghouse PWRs) and developing models that constitute good approximations to the plants in each class. The development of such a generalized model for a class of designs is not in the scope of current work. These models would depict the logical interrelationship of frontline and support system functionabilities and the achievable levels of the safety objectives. The dependence of the frontline systems on the support systems could be generalized by assuming that the frontline systems depend on the whole support system. An example is the model developed for the Limerick. Generating Station (LGS) in the course of the review[4] of the LGS-PRA.[5] Given such a model and an "objective" function (e.g., cost), a set of systems performance criteria consistent with the given set of top level safety criteria could be developed. This set of performance criteria would be representative of all the plants in each class. The "objective" function would, in general, express the degree of difficulty in achieving a particular level of system reliability (for plants under design) or of a deviation from an existing level (for existing plants).

This set of system reliability criteria would thus represent design "aspirations" toward which a specific plant would be designed (new plant) or backfitted (existing plant). In particular, for existing plants realistic and feasible backfitting options would be examined on the basis of the established reliability "aspirations" and the existing systems.

Compliance with the system performance criteria for a specific plant would not, however, guarantee compliance with the top level safety criteria. A detailed plant-specific model would be necessary for the latter. From this model the specific levels of achievement in the various safety objectives (i.e., core damage frequency, acute and latent fatalities) and the associated

*Frontline systems are those that directly affect the performance of safety functions. Support systems are those that affect the functioning of the frontline systems.

cost would be determined, and a decision would be made on the basis of these specific results. We believe, nevertheless, that a plant specific design (or backfit) that complies with the safety criteria will be reached much faster if the starting point is based on the developed system performance requirements.

In short, while we do not have clear answers to Questions #2 and #3 at this time, we investigated the technical feasibility of the development of a set of system reliability performance requirements that are consistent with an agreed upon set of general objectives or global risk indices (safety and cost) and which are valid for a specific nuclear power plant design. The question, however, of whether generalized models representing classes of nuclear power plants exist, or of whether different models could result in similar system reliability performance requirements remains open. If such sets of generalized system criteria exist, they will constitute "aspirations" on the basis of which plant specific designs will be developed (or changed) in order to achieve the general safety objectives. The degree of satisfaction (compliance) of these safety objectives will, however, be determined with the help of a plant-specific model and along with economic considerations.

A.2 Cost Considerations

The general objective of the program is to develop a methodology for the determination of self-consistent and balanced reliability criteria among safety functions, plant systems, major components, and possibly operational practices in the presence of global (top level) safety criteria or "safety goals". The methodology should, therefore, be able to "transform" general safety goals (related to core damage frequency, expected acute and latent fatalities) into reliability requirements for the various systems and major components that affect (through their potential failures) the levels and the frequencies of the various undesirable consequences (e.g., core damage, acute and latent fatalities).

The proposed methodology addresses this problem as a general optimization problem. The levels and frequencies of the various undesirable consequences that could be realized following an accident (a combination of failures) in a nuclear power plant, can be expressed as mathematical functions of the system (component) reliabilities (see Section A.3.1). The global safety criteria can be seen as constraints on the undesirable consequences. The whole problem then transforms into one of identifying the reliabilities of systems that satisfy the constraints in some "optimum" way. The next two steps in the formulation of the problem are then: 1) definition of the mathematical relationships between the global constraints and the system reliabilities; and 2) definition of the "optimality" condition under which the problem will be solved.

The mathematical models which provide the necessary relationships between the system reliabilities and the global risk indices are provided by the various probabilistic risk assessment (PRA) studies. This part of the problem will be discussed in Section A.3.1. Here we present a preliminary, mostly qualitative, discussion of the "optimality" condition, and introduce the concept of cost.

Given the mathematical relationships between the system reliabilities and the undesirable consequences as well as the constraints on these consequences

(safety criteria), we could try to identify the set of system reliabilities (solution) that yield consequences equal to the safety criteria. This problem could have zero, one, or many solutions. Furthermore, there are a large number of solutions that satisfy the constraints (i.e., that yield consequences smaller than the safety criteria). Which of these solutions is the preferred one? If there were no constraints on the achievability of the various system reliability levels, we would choose the solution which results in the lowest possible consequences. In the limit, this would have implied zero consequences achieved through perfect system reliabilities. Of course this is not possible, since a particular level of system reliability is achieved through the expenditure of resources and in addition there are technological constraints on the achievable levels of system reliability. Thus, the lower the implied consequences, the higher the required reliability levels and the higher the needed resources or "cost" of the solution. The "cost" implied by a particular reliability level is, therefore, a necessary ingredient in our allocation problem, and the driving force that constrains the solution from reaching the highest (mathematically or technologically) achievable system reliabilities. The introduction of the concept of cost provides a possible condition of optimality. That is, given the set of solutions that satisfy the constraints, the preferred solution is the one that minimizes the "cost". This approach has, nevertheless, a number of problems. First, the specification of a reliability cost function is fraught with uncertainty. Second, even if reliability cost functions were available, their indiscriminate use in optimality conditions could obscure important aspects of the problem by masking implied tradeoffs among the global risk indices, as well as among the global risk indices and the cost. We will elaborate further on these points with help of a simple example.

Let us consider a simple system consisting of two components connected in series (see Figure A.1). This arrangement can be considered as an idealized representation of the safety systems of a nuclear power plant with components 1 and 2 corresponding to the decay heat removal system and the reactor protection system, respectively. Whenever a challenge to these two systems (an accident initiator) coincides with either of them being unavailable, an accident occurs that results in core damage (C_d) and possibly in acute fatalities (A) and/or latent fatalities (L). These consequences can be expressed as functions of the decay heat removal system and the reactor protection system unavailabilities (x_1,x_2) as follows.

$$C_d = f[x_1 + x_2 - x_1x_2] \tag{A.1}$$

$$A = f[\alpha_1x_1x_2 + \alpha_2x_2(1-x_1) + \alpha_3(1-x_2)x_1] \tag{A.2}$$

$$L = f[\beta_1x_1x_2 + \beta_2x_2(1-x_1) + \beta_3(1-x_2)x_1] \tag{A.3}$$

where

C_d = the frequency of core damage

A = the expected number of acute fatalities

L = the expected number of latent fatalities

f = the frequency of the accident initiator

α_i = coefficients determining the expected number of acute fatalities given an accident initiator and a particular combination of system failures, i = 1, 2, 3

β_i = same as α_i for latent fatalities, i = 1, 2, 3.

The coefficients α_i, β_i depend, in general, on the containment response, the population and weather characteristics of the site.

Let (C_d*, A*, L*) be a set of constraints (global safety criteria) on the three measures of the undesirable consequences. Our problem reduces in this case to one of determining the unavailabilities (x_1, x_2) that satisfy the constraints

$$C_d \leq C_d^* \tag{A.4}$$

$$A \leq A^* \tag{A.5}$$

$$L \leq L^* \tag{A.6}$$

and that are at the same time "optimum" in some sense (yet to be defined).

First, we try to determine all possible pairs (x_1, x_2) that satisfy the constraints. Assuming that there are some lower limits (x_1°, x_2°) that correspond to the lowest technologically achievable unavailabilities, the set of pairs (x_1, x_2) that satisfy Eqs. (A.1)-(A.3) defines a subspace E in the two-dimensional Euclidean space R_2 (see Figure A.2). The contour of subspace E is defined by the various constraints. The boundaries OD and OA are defined by the technological limits on x_2 and x_1, respectively. The boundary ABCD is defined by the constraints (A.4)-(A.6) where the assumption that $x_1 x_2 \ll x_1 + x_2$ was made.* AB corresponds to the acute fatalities constraint (A.5). BC corresponds to the core damage frequency constraint (A.4). CD corresponds to the latent fatalities constraint (A.6). Every point in the feasible subspace E satisfies the constraints (A.4)-(A.6), but which one is the "best" solution? Obviously, in the absence of any other constraints the "best" solution is the point (x_1°, x_2°) which achieves the lowest possible undesirable consequences (C_d, A, L). This solution corresponds to an ALAPA (as low as possibly achievable) policy which does not consider the "cost" or more generally the degree of difficulty in achieving the unavailability levels (x_1°, x_2°). In general, we may assume that the lower the unavailability of the system the higher the "cost" or the degree of difficulty in achieving it. In that sense, we may be interested in higher unavailabilities that still satisfy the constraints but which are a compromise between competing constraints.

The boundary "ABCD" exhibits an interesting property in that among the points in the set E all the possible points (x_1, x_2) that satisfy the constraints and contain the highest values of the unavailabilities belong to the subset "ABCD". In mathematical form, for every point (x_1', x_2') on ABCD the boundary ABCD has a property that

This assumption is valid for the range of the unavailability values (x_1, x_2) that satisfy the constraints (C_d, A*, L*) considered in this example and when the events are independent. See Section 4.2 and Section A.4.

$$x_1' \geq x_1 \qquad (A.7)$$

$$x_2' \geq x_2$$

with at least one inequality strictly holding.

The points in the boundary "ABCD" constitute solutions of an AHAPA (as high as possibly allowable) policy and they provide the highest possible unavailabilities that satisfy the constraints. Now, we may ask; Is (x_1°, x_2°) more preferred to any point in the boundary "ABCD"? This question is equivalent to: Is the difference in "cost" between a point in ABCD and (x_1°, x_2°) worth the corresponding difference in the three measures of the undesirable consequences (C_d, A, L)?

The establishment of such tradeoffs (via a preference assessment) among the core damage frequency, the health consequences and the "cost" or the degree of difficulty in achieving the system unavailability levels is outside the scope of this current study. The above discussion indicates, however, the need for a "cost" consideration lest the solution of the problem degenerate into an ALAPA solution, that is, "the unavailabilities should be equal to the lowest technologically achievable".

A possible alternative is to confine our problem to defining the boundary ABCD and leave it to appropriate decision makers to decide which point on this boundary is the preferred one. The rationale is that the points on ABCD represent the "highest" allowable unavailabilities. There is, however, a drawback. There might be other points in E not belonging to ABCD and yet being preferable to the points of ABCD. For example, if we assume for illustration purposes that the cost function has the form

$$G(x_1,x_2) = 1/x_1 + 1/x_2 \qquad (A.8)$$

then the "isocost" curves, that is, the locus of the points that have the same cost, have the form shown in Figure A.3. Points C, C' and C" are characterized by the same cost. Points C and C" belong to the ABCD boundary, yet point C' is clearly preferred to points C and C" because it corresponds to lower values of all three consequences (C_d, A, L). One possible approach to this problem is to ask for the point that minimizes the cost function $G(x_1,x_2)$ and at the same time satisfies the constraints. The solution of this problem is the point at which an "isocost" curve is tangent to the boundary of space E (let B be this point in Figure A.3). Point B could have been determined directly by solving the single-objective optimization problem* of minimizing $G(x_1,x_2)$ subject to the constraints (A.4)-(A.6). Since, however, the function $G(x_1,x_2)$ is generally not well known (at least for the purposes of this study) and sensitivity studies (with different cost functions) are desirable, computational effort might be saved by first determining the boundary ABCD and then identifying the point (on it) that minimizes a cost function. The boundary ABCD can be used later with different cost functions. In this way, potential problems owing to imprecision or even inappropriateness of the cost function are partially avoided.

There is, however, an important issue that the above procedure does not address. This has to do with the ambiguity and/or associated trade-offs in the safety criteria (constraints). For example, point B in Figure A.3

satisfies the constraints and minimizes the cost function $G(x_1,x_2)$. Point C', however, achieves a lower core damage frequency, less acute and latent fatalities albeit at a higher cost. It might be desirable to provide the appropriate decision makers with choices like these instead of assuming that a particular set of safety criteria is permanently defined and no deviation from these criteria is advisable or desirable. In order to define a set of solutions that offers this greater flexibility and range for decision making, we must identify the subset F of R_2 that contains the "noninferior" solutions. A feasible solution to a multiobjective optimization problem* is noninferior if there exists no other feasible solution that will yield an improvement (reduction) in one of the objectives without causing a degradation (increase) in at least one other objective. (This will be formally stated in mathematical terms in Subsection A.3.3.)

The selection of the most preferred point in F will then be left to appropriate decision makers who will establish value tradeoffs (make decisions) among the four variables of the problem.

In conclusion, there are three general approaches to the problem. These approaches, in order of increasing flexibility for decision making and possibly increasing complexity, are:

1) Assume a cost function and solve the single-objective optimization problem of minimizing cost, subject to the safety criteria constraints.

2) Do not consider a specific cost function but identify the set of "maximum" solutions that satisfy the safety criteria constraints. (Maximum in the sense that for a solution point that satisfies the constraints there is no other solution in the set that has higher or equal unavailability.)

3) Assume a cost function and do not consider a specific set of safety criteria and identify the set of all solutions that are noninferior. That is, identify all solutions that cannot be improved in any one of the objectives without degrading some other objectives.

The first two approaches correspond to a situation in which performance standards have been set for the nuclear plants on some rational basis and the cost question is examined posterior to this standard (safety criteria) setting. Obviously, these approaches examine only those alternatives that satisfy the specific (preset) standards. The third approach, in contrast, does not assume a preset set of safety criteria but rather sets the stage for a "decision making" procedure that allows for cost considerations in parallel to the other performance indices. This approach selects--on a technical basis--from a given set of alternatives those that need be further examined by appropriate policy makers to determine the preferred one. It is this third approach that we have chosen to follow and which we discuss further in the following subsection.

*In a single-objective optimization problem there is only one objective function to be optimized (e.g., minimized) whereas in a multiobjective problem there are multiple objective functions to be optimized simultaneously. See Section A.3.3.

A.3 Mathematical Definition of the Methodology and Model Description

In Section 2 and the first two subsections of this section, we discussed the basic principles and gave a qualitative description of the proposed methodology for the decomposition of the global safety criteria. In this section the formal mathematical models are defined. In particular, in Section A.3.1 we present the PRA model that provides the functional relationship of the consequence variables (core damage, acute and latent fatalities) with the system unreliabilities (decision variables). In Section A.3.2 we discuss various reliability cost models and in Section A.3.3 we present the formal form of the multiobjective optimization problem and methods for its solution.

A.3.1 PRA Models

The current PRA models provide the most comprehensive description of the relationships between the safety undesirable consequences and the reliabilities of the various safety functions, systems, and major components in a nuclear power plant. For this reason and despite some drawbacks and limitations[6,7] the PRA models provide the best available basis for risk related decision making.

The relationship between the undesirable consequences (e.g., core damage frequency, acute fatalities, latent fatalities) of an accident in a nuclear power plant and the reliability measures of the various systems can be presented in matrix formalism[8,4] as follows:

Let

$h_i (i=1,\ldots,N)$ denote N levels of the undesired consequence (acute, latent fatalities) that forms the base of the risk criterion,

and

$w_i(h_i)$ $(i=1,\ldots,N)$ denote the frequency of the ith level of consequence h; the following row vector is then defined,

$$\underline{w}(\underline{h}) = [w_1(h_1), w_2(h_2), \ldots, w_N(h_N)] \qquad (A.9)$$

Let

R_r $(r=1,2,\ldots K)$ denote the K types of radioactivity releases, each of which uniquely defines the probability that a particular level of consequence $\underline{h}$ will occur at a given site,

and

s_{rn} denote the conditional probability that, given release R_r, the nth level of consequence h_n will occur,

then the following Site Matrix can be defined:

$$\underline{S}=[s_{rn}]\text{: KxN matrix.} \qquad \text{(A.10)}$$

Let

D_j (j=1,2,...,J) denote the J types of plant-damage states each of which uniquely defines the conditional probability that a particular radioactivity release R_r will result,

and

c_{jr} denote the conditional probability that given plant-damage state j, the rth radioactivity release will result.

The following Containment Matrix can then be defined:

$$\underline{C}=[c_{jr}]\text{: JxK matrix.} \qquad \text{(A.11)}$$

Let

I_i (i=1,2,...,I) denote the I types of accident initiators each of which uniquely defines the conditional probability that a particular plant-damage state will result from the accident,

and

m_{ij} denote the conditional probability that given initiator I_i, the jth plant-damage state will result. The m_{ij} are functions of the unavailabilities of safety functions, systems, subsystem, or components, i.e., $m_{ij} = f_{ij}(x_1,x_2,...,x_n)$.

The following Plant-Damage Matrix can then be defined:

$$\underline{M} = [m_{ij}]\text{: IxJ matrix.} \qquad \text{(A.12)}$$

Finally, let

f_i (i=1,2,...,I) denote the frequency of the ith accident initiator (internal and external).

The following initiator row-vector can then be defined:

$$\underline{f} = [f_1,f_2,...f_I]\text{: 1xI vector} \qquad \text{(A.13)}$$

Given these definitions, it can be shown that the consequence frequency vector $\underline{w}(\underline{h})$ is given by

$$\underline{w}(\underline{h}) = \underline{f}\,\underline{M}\,\underline{C}\,\underline{S} \qquad \text{(A.14)}$$

Further we have:

Core damage frequency: $C_d = \underline{f}\,\underline{M}\,\underline{u}$ (A.15)

where $\underline{u} = [1,1,\ldots,1]^T$ (column vector).

Expected acute fatalities: $A = \underline{w}(\underline{a})\underline{a}$ (A.16)

where

$\underline{a} = [a_1,a_2,\ldots,a_N]^T$ (column vector of the N levels of acute fatalities)

and $\underline{w}(a) = \underline{f}\,\underline{M}\,\underline{C}\,\underline{S}(\underline{a})$ (see A.16) (A.16a)

with $\underline{S}(\underline{a})$ the site matrix for acute fatalities.

Expected latent fatalities: $L = \underline{w}(\underline{\ell})\underline{\ell}$ (A.17)

where $\underline{\ell} = [\ell_1,\ell_2,\ldots,\ell_N]^T$ (column vector of the N levels of latent fatalities)

and $\underline{w}(\underline{\ell}) = \underline{f}\,\underline{M}\,\underline{C}\,\underline{S}(\underline{\ell})$ (see A.16) (A.17a)

with $\underline{S}(\underline{\ell})$ the site matrix for latent fatalities.

Eqs. (A.15)-(A.17) constitute the three general constraint functions of our problem. They relate the three measures of the undesirable consequences (core damage frequency, expected acute, and expected latent fatalities) with the unavailabilities of the systems of a nuclear power plant. The latter define the elements of the plant damage matrix $\underline{M}$.

A.3.2 Reliability Cost Functions

The current PRA models do not take into consideration the costs related to the reliability of the plant. This is because the PRA is used as an evaluation methodology of a given plant.* If the PRA model is to be used as a model for allocating safety criteria or identifying the "best" way of improving reliability to satisfy the safety criteria, the cost involved becomes an important element, as discussed in Subsection A.2. The type of cost we are interested in in this study is that associated with achieving a particular level of reliability for safety related systems.

In general, a reliability cost function of a single component is assumed to satisfy the following basic properties:[9]

1. Cost is a monotone increasing function of reliability.
2. Derivative of cost with respect to reliability is a monotone increasing function of reliability.
3. Cost of a high reliability component is very high.

*There is a growing interest in utilizing PRA results for cost-effective plant modifications, e.g., Ref. 10.

These three properties express intuitively appealing characteristics of the cost function, supported by experience, which, in addition, result in some analytical convenience.

The first property that cost is a monotone increasing function of reliability is logical in that it represents a correct trend which realistic cost functions would exhibit. The second property is more restrictive than the first property and generally applies only to a "theoretical" (i.e., elementary) component. The cost functions for components existing in reality would not necessarily satisfy this property. The applications presented in this report have employed cost functions that both do and do not satisfy this property. The third property mentioned above implies infinite cost at zero unreliability. It is always assumed in this work that there is a nonzero lower limit in the achievable unreliability set by technological considerations.

Some of the reliability cost functions used in the reliability literature are the following [expressed in terms of the unreliability or unavailability of a component, x_i, and denoted by $g_i(x_i)$]:

1. $g_i(x_i) = a_i \exp(b_i/x_i)$, $a_i, b_i > 0$

2. $g_i(x_i) = a_i \tan \frac{\pi}{2}(1-x_i) + b_i$, $a_i, b_i > 0$

3. $g_i(x_i) = a_i/x_i + b_i$, $a_i, b_i > 0$

4. $g_i(x_i) = -a_i \ln x_i + b_i$, $a_i, b_i > 0$.

The four reliability cost models listed above give the cost of achieving unavailability level x_i for component i, and satisfy the three basic properties mentioned above. The parameters a_i and b_i are to be determined by field cost data.

Once reliability cost functions are known for components, our expression for the total cost is

$$G = \sum_{i=1}^{n} g_i(x_i) \qquad \text{(A.18)}$$

where n is the number of components.

A.3.3 Multiobjective Optimization Model

An optimization problem has to deal with finding "optimum" solutions of (an) objective function(s) and corresponding decision variables satisfying constraints, if there are any. Constraints can be imposed both on the objective function(s) and on the decision variables.

The objective functions and decision variables which we are interested in would be the following:

Objective functions: $\underline{Z}$

1. Core damage frequency, C_d in Eq. (A.15)
2. Expected acute fatalities (individual, societal), A in Eq. (A.16)
3. Expected latent fatalities (individual, societal), L in Eq. (A.17)
4. Cost (of achieving the reliabilities), G in Eq. (A.18)

Decision variables: $\underline{x}$

1. Unavailabilities of safety functions, systems, and components including human errors (depending on the level of resolution of the plant model) (affect the elements of $\underline{M}$ in A.15-A.17)
2. Initiator frequencies (vector $\underline{f}$ in A.15-A.17)
3. Containment failure probabilities (affect elements of $\underline{C}$ in A.16-A.17)
4. Site parameters (affect the elements of $\underline{S}$ in A.16-A.17)
5. Emergency planning parameters (evacuation, sheltering, and other parameters affecting the elements of $\underline{S}$ in A.16-A.17)

It is worthwhile to mention that not every item in the list above has to be considered. This will depend on the level of detail and on the purposes of the analysis. For example, items from (2) to (5) in decision variables may be considered as given constants in the first phase of the analysis.

A.3.3.1 Problem Definition

Multiobjective programming deals with optimization problems with two or more objective functions. The multiobjective optimization (also called vector optimization) problem is written as[11]

$$\text{Minimize } \underline{Z}(\underline{x}) = [Z_1(\underline{x}), Z_2(\underline{x}), \ldots, Z_p(\underline{x})] \text{ subject to } \underline{x} \in F_d \qquad (A.19)$$

in which $\underline{Z}(\underline{x})$ is a p-dimensional vector composed of the objective functions. F_d is the feasible region in decision space. Note that the individual objective functions $Z_i(\underline{x})$ are merely listed. They are not added, multiplied, or combined in any way.

The notion of "optimality" in single-objective optimization problems must be dropped in multiobjective problems because a solution which minimizes one objective will not, in general, minimize any of the other objectives. A new concept called "noninferiority" (or "nondominance") will serve a similar but less limiting purpose for multiobjective problems.

A solution $\underline{x}$ is noninferior if there exists no feasible $\underline{x}'$ such that

$$Z_k(\underline{x}') \leq Z_k(\underline{x}),\ k = 1,2,\ldots,p \qquad (A.20)$$

where the strict inequality holds for at least one k. If such a feasible $\underline{x}'$ exists, then $\underline{x}$ is inferior. $\underline{Z}(\underline{x})$ corresponding to a noninferior solution $\underline{x}$ are called noninferior objective functions.

Figure A.4 illustrates the definition of noninferiority for a two-dimensional case. A set of feasible solutions in objective space for a two-objective minimization problem is shown. Point C is inferior to B and D since B gives smaller Z_2 without increasing Z_1 and D gives smaller Z_1 without increasing Z_2. Point A (similarly D and B) is noninferior since we cannot decrease Z_1 without increasing Z_2 and vice versa. Noninferior solutions such as points A, D and B (actually any point on the crosshatched curve along A, D, B in Figure A.4) are of interest.

For our reliability/risk allocation problem, Z_1 would be, for example, the core damage frequency and Z_2 the cost.

A.3.3.2 Solution Techniques

Solution techniques for multiobjective optimization problems can be divided broadly into two categories: Generating techniques and preference-oriented techniques. The generating techniques emphasize the full exposition of information about a multiobjective problem that allows a decision maker to understand the range of choice and the trade-offs among alternatives. They do not require explicit articulation of a decision maker's preference or value judgments.

The techniques that incorporate preferences, however, require that decision makers articulate their preferences and value judgments and pass that information on to the analyst, in advance of the analysis or during the analysis.

(1) Generating Techniques

These techniques try to identify the noninferior solution set of decision variables and of corresponding objective functions. No explicit preferences of a decision maker are required. Most of these methods are based on repeated applications of the single-objective programming techniques. The most widely used techniques in this category are:

i) The Weighting Method

$$\text{Minimize } z(\underline{x}) = \sum_{k=1}^{p} w_k Z_k(\underline{x})$$

subject to $\underline{x} \in F_d$, $\underline{w} \geq 0$.

The w_k's are varied parametrically to trace out noninferior solutions.

ii) The Constraint Method

Minimize $z(\underline{x}) = Z_h(\underline{x})$

subject to $\underline{x} \in F_d$,

$$Z_k(\underline{x}) \leq \varepsilon_k, \; k = 1,2,\ldots,p, \; k \neq h.$$

The ε_k's are varied parametrically to trace out noninferior solutions. The choice of $Z_h(\underline{x})$ as the objective function is arbitrary. Any one of $Z_k(\underline{x})$, $k = 1,2,\ldots,p$ can serve as the objective function.

(2) Preference-Oriented Techniques

These techniques determine the best-compromise solution in some sense. They require articulation of a decision maker's preferences in advance or progressively. For chosen preferences, the problem becomes a single-objective programming problem. These techniques can be grouped in two categories: i) Noniterative methods, and ii) Iterative methods. The details can be found in Refs. (11), (12), and (13).

A.3.3.3 Problem Statement

Our specific allocation problem takes the form

$$\text{Minimize } \underline{Z}(\underline{x}) = [C_d, A, L, G] \tag{A.21}$$

subject to $x_i \in F_{di}$, all i,

where C_d, A, L, and G are defined in Eqs. (A.15), (A.16), (A.17), and (A.18), respectively.

This problem can be solved by one of the techniques described above, e.g., the weighting method or the constraint method. A computer program RAMOP (Reliability Allocation by Multi-Objective Programming) was developed in this study for numerical solutions to multiobjective optimization problems of the form in Eq. (A.21). RAMOP employs the constraint method and calls a NAG subroutine.[14] The subroutine is a standard single-objective optimization routine and is based on the augmented Lagrangian method.

A.3.3.4 Examples

Two simple examples are presented here to demonstrate the model presented in previous subsections. The examples shown here are simple enough so that they admit analytical solutions and graphical representations and provide useful insights to the characteristics of the allocation problem. A much more complex and realistic problem with numerical solutions is presented in Appendix B.

Example 1: Allocation model for Figure A.5

Minimize $\underline{Z}(x_1,x_2) = [Z_1,Z_2]$

subject to $x_1,x_2 \in (0,1)$

where $Z_1 = f_1x_1x_2$ is the core damage frequency and f_1 is the accident initiator frequency and x_1 and x_2 represent system unavailabilities.

$Z_2 = a_1/x_1 + a_2/x_2$ represents the cost of improving x_1 and x_2; a_1 and a_2 are cost coefficients.

This multiobjective optimization problem can be solved by the constraint method as follows:

Minimize $Z_2 = a_1/x_1 + a_2/x_2$

subject to $x_1, x_2 \in (0,1)$

$$Z_1 = f_1x_1x_2 \leq \varepsilon_1.$$

Define the Lagrangian function $L = Z_2 + \lambda(Z_1-\varepsilon_1)$ and assume optimum solutions are away from lower (0) and upper (1) limits.
Then optimum solutions must satisfy the following first-order necessary conditions:[11,15]

i) $\frac{\partial L}{\partial x_1} = 0$

ii) $\frac{\partial L}{\partial x_2} = 0$

iii) $\lambda \geq 0$

iv) $\lambda(Z_1-\varepsilon_1) = 0 \rightarrow Z_1-\varepsilon_1 = 0$ from a noninferiority condition $\lambda \neq 0$.

After some algebraic manipulations we have solutions:

$x_1 = \sqrt{\varepsilon_1a_1/f_1a_2}$

$x_2 = \sqrt{\varepsilon_1a_2/f_1a_1}$.

The above solutions (parametric in ε_1) also satisfy the second-order sufficiency condition for optimality, i.e., the Hessian matrix is positive definite on the tangent subspace of the active constraints.Thus, we have the following noninferior solutions:

$x_1 = \sqrt{\varepsilon_1a_1/f_1a_2}$

$x_2 = \sqrt{\varepsilon_1a_2/f_1a_1}$

$$Z_1 = \varepsilon_1$$

$$Z_2 = 2\sqrt{f_1 a_1 a_2/\varepsilon_1}.$$

Noninferior Z_1 and Z_2 satisfy the following relation which is also shown in Figure A.7:

$$Z_1 Z_2^2 = 4 f_1 a_1 a_2 = \text{constant}.$$

Note that the ratio of the allocated system unavailabilities, $x_1/x_2 = a_1/a_2$, is independent of the accident initiator frequency and of the safety goal (ε_1). It depends only on the ratio of the cost coefficients such that the more costly system is allocated a larger share of unavailability. The absolute values of the unavailabilities do depend on the safety goal level and on the initiator frequency.

Example 2: Allocation model for Figure A.6

Minimize $\underline{Z}(x_1,x_2) = [Z_1,Z_2]$

subject to $x_1,x_2 \in (0,1)$

where $Z_1 = f_1 x_1 + f_2 x_2$ is the core damage frequency and f_1 and f_2 are the frequencies of two different accident initiators.

$Z_2 = a_1/x_1 + a_2/x_2$ is the cost, as before.

By similar procedures as in Example 1, we have the following noninferior solutions:

$$x_1 = \frac{\varepsilon_1}{f_1} \frac{1}{1 + \sqrt{\frac{a_2 f_2}{a_1 f_1}}} \qquad x_2 = \frac{\varepsilon_1}{f_2} \frac{1}{1 + \sqrt{\frac{a_1 f_1}{a_2 f_2}}}$$

$$Z_1 = \varepsilon_1$$

$$Z_2 = \frac{1}{\varepsilon_1} \left(\sqrt{f_1 a_1} + \sqrt{f_2 a_2}\right)^2$$

Noninferior Z_1 and Z_2 satisfy the following relation which is also shown in Figure A.8:

$$Z_1 Z_2 = \left(\sqrt{f_1 a_1} + \sqrt{f_2 a_2}\right)^2 = \text{constant}.$$

Again, we see that when we form the ratio of the unavailabilities, it is independent of the safety goal level, i.e.,

$$x_1/x_2 = \sqrt{a_1/a_2}\ \sqrt{f_2/f_1}\ .$$

It also shows the same qualitative dependence on the ratio of the cost coefficients as in Example 1. The dependence on the ratio of the initiator frequencies agrees with our intuition that the allocated unavailabilities will scale inversely with the accident initiator frequencies.

A.4 Analysis of the Rare Event Approximation for a Simple Model System

The error incurred in the reliability allocation for a simple model system by assuming that the rare event approximation is valid is examined in this subsection.

Consider two independent events with corresponding demand unavailabilities X_1 and X_2. A top event, described by an objective function Z_1, occurs if either of the independent events occurs. If f denotes the frequency of an initiating event, then

$$Z_1 = f(X_1 + X_2 - X_1X_2). \tag{A.22}$$

Some preliminary heuristic remarks are in order. If Z_1 is required to satisfy a constraint $Z_1 = \epsilon$, then if $\epsilon/f \ll 1$, one would expect the "solution range" for X_1, X_2 to be such that X_1X_2 is much smaller than both X_1 and X_2. On the other hand, if $\epsilon/f < 1$, then solutions $X_1 < 1$ and $X_2 < 1$ are possible and therefore the term X_1X_2 cannot be ignored relative to $X_1 + X_2$.

Let us now find the optimum solutions X_1, X_2. We will do this by minimizing the cost function (see Section A.3.2 for a discussion of cost functions)

$$Z_2 = -a_1 \ln X_1 - a_2 \ln X_2, \tag{A.23}$$

subject to the constraint $Z_1 = \epsilon$.

As in Section A.3.3.4 we introduce a Lagrange parameter λ and readily find the optimum solutions from

$$f(1 - X_2) = \frac{a_1\lambda}{X_1}$$

$$f(1 - X_1) = \frac{a_2\lambda}{X_2} .$$

These equations imply that

$$X_1 = \frac{\xi X_2}{1 + (\xi - 1) X_2} \tag{A.24}$$

where $\xi \equiv a_1/a_2$.

By using Eq. (A.24) in the constraint on Z_1, the following equation for X_2 is obtained:

$$X_2^2 + [(\xi - 1)\frac{\varepsilon}{f} - (\xi + 1)]X_2 + \frac{\varepsilon}{f} = 0.$$

Hence

$$X_2 = \frac{1}{2}\left[(\xi + 1) + (1 - \xi)\frac{\varepsilon}{f} - \sqrt{[(\xi - 1)\frac{\varepsilon}{f} - (\xi + 1)]^2 - \frac{4\varepsilon}{f}}\right].$$

(The positive root is rejected since it does not give a physically meaningful result.)

If the cost coefficients are equal, $a_1 = a_2$, then $\xi = 1$ and we have

$$X_2 = 1 - \sqrt{1 - \varepsilon/f}$$

$$= X_1 \text{ (by symmetry).} \qquad \text{(A.25)}$$

At this point, we note that the solution to the approximate optimization problem with

$$Z_1 \approx Z_1^A = f(X_1 + X_2)$$

is

$$X_1^A = \frac{\varepsilon}{f}\frac{a_1}{a_1 + a_2}, \quad X_2^A = \frac{\varepsilon}{f}\frac{a_2}{a_1 + a_2}.$$

Thus, if $a_1 = a_2$,

$$X_1^A = X_2^A = \frac{1}{2}\frac{\varepsilon}{f}. \qquad \text{(A.26)}$$

We see that Eq. (A.26) is the first order (in ε/f) approximation to Eq. (A.25). Further, we can see how the approximation breaks down as $\varepsilon/f \to 1$. For $\varepsilon/f = 1$, the extreme case, Eq. (A.26) underestimates X_1, X_2 by a factor of 2. For $\varepsilon/f = 0.5$, Eq. (A.26) underestimates the exact solution, Eq. (A.25) by 14%, which is a small error.

This observation tells us that the allocated unavailabilities ("aspiration" levels) obtained by using the rare event approximation are conservative in the sense that the aspiration levels are lower than those which are obtained by using the exact expression, Eq. (A.22). Furthermore, the error becomes very small in the range of $\varepsilon/f \approx 10^{-4} - 10^{-2}$ in which we are interested.

Similar results were obtained* for the cost function

$$Z_2 = \frac{a_1}{X_1} + \frac{a_2}{X_2}.$$

*The calculations were performed by C. K. Park.

The results also showed that even for the case $a_1 \neq a_2$ the rare event approximation is a good approximation (as noted above) for this model even when

$$10^{-3} < \frac{a_1}{a_2} < 10^{3}.$$

The results obtained in this subsection, while obtained on a simple model system, give insights and lend confidence to the range of applicability of the rare event approximation in the allocation problem.

A.5 Specification of Point Values as Mean Values

The methodology presented in this appendix and proposed for the reliability and risk allocation was developed under the implicit assumption that the allocated (calculated) reliabilities are point values unambiguously defined or, more desirably, of the same characteristic as that of the top level safety criteria (global measures). In other words, since the top level criteria (i.e., core damage frequency, acute fatalities, and latent fatalities) are mean (expected) values as in most of the proposed safety goals in the literature, it is desired that the allocated component reliabilities calculated by the proposed methodology are also mean values.

This desirable "closure" property holds for the PRA models in a fairly broad generality. The PRA models based on event/fault tree analysis are multilinear in the reliabilities (or unavailabilities) if it is assumed that the basic events are statistically independent. When there are dependent events (common cause failures), the β-factor approach[16] allows, to a good approximation, the PRA models to be recast also in multilinear forms with statistical independence. In this case of multilinearity and statistical independence, it is easy to show that the closure property holds, i.e., the top level criteria are also mean values when the allocated component reliabilities are mean values, regardless of the distributions.

For the reliability cost functions in Section A.3.2, the closure property holds in the coefficients a_i and b_i, but not in the unavailability X_i. Nevertheless, we can say that the total reliability cost G in Eq. (A.18) is a "mean-point" value which corresponds to the mean unavailabilities in the PRA model's part of the allocation methodology.

The closure property, however, does not hold when the PRA models are refined to consider the so-called "state-of-knowledge" dependency.[17] The incorporation of the "state-of-knowledge" dependency in the PRA models leads no longer to multilinear forms, but to forms of higher order polynomials, e.g., X_i^2 for some component i. However, consideration of this type of dependency can be postponed and taken into account later in the uncertainty analysis.

Several approaches to addressing uncertainties in the global measures and in the allocated reliabilities, due to uncertain parameters in the models, are described in Appendix D.

Figure A.1 Two component series systems.

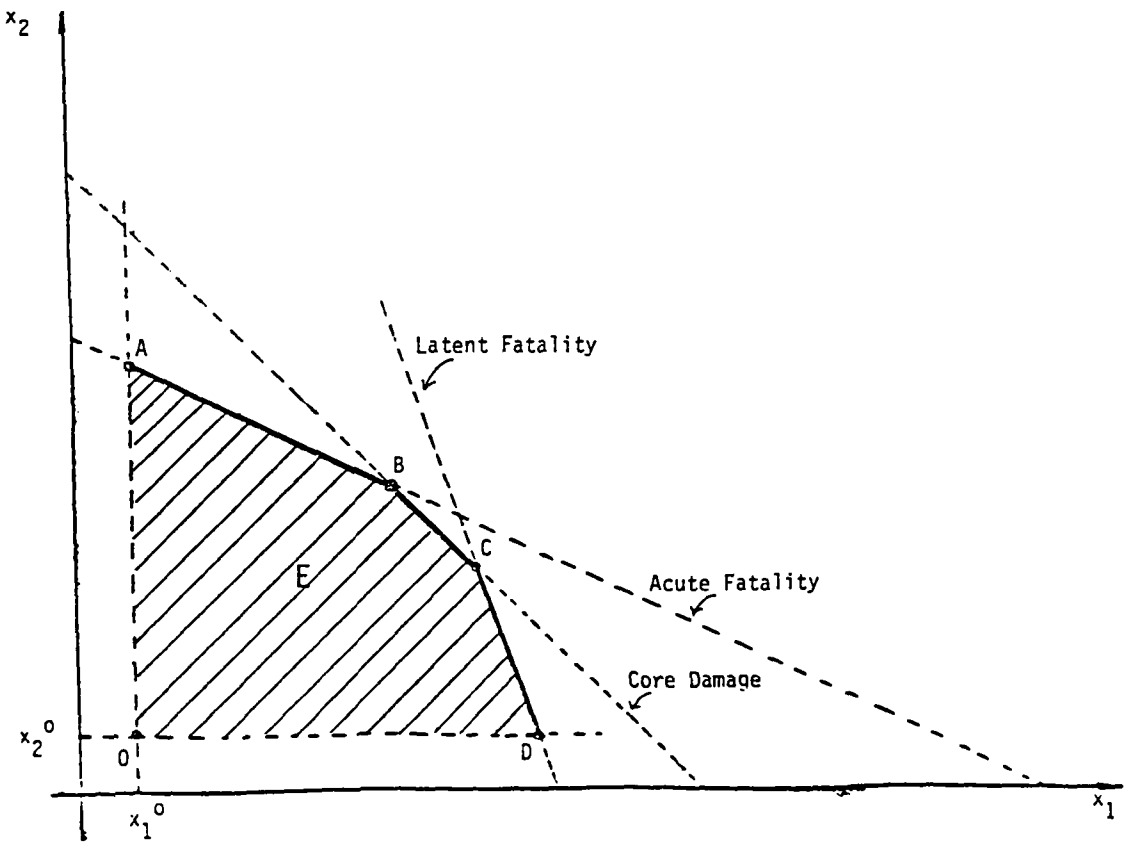


Figure A.2 Feasible solution in decision variable space for example problem.

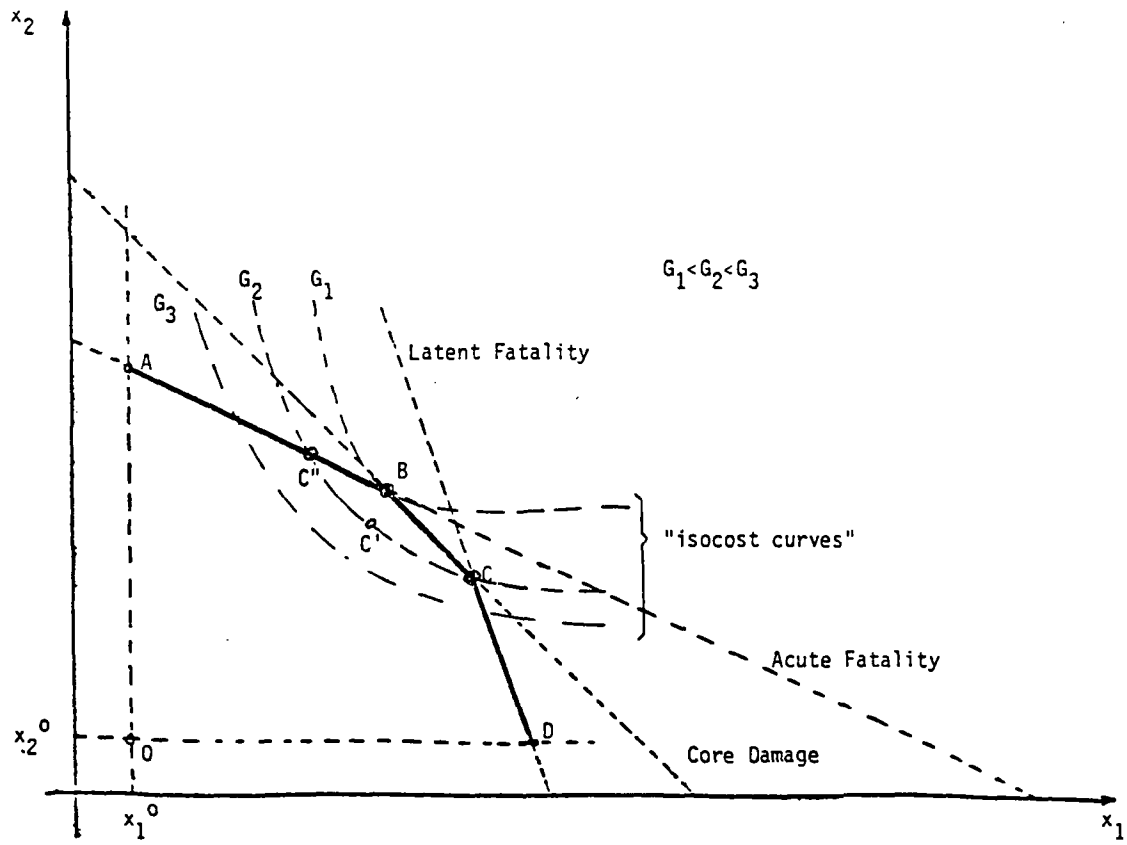


Figure A.3 Feasible solution in decision variable space for example problem with isocost curves.

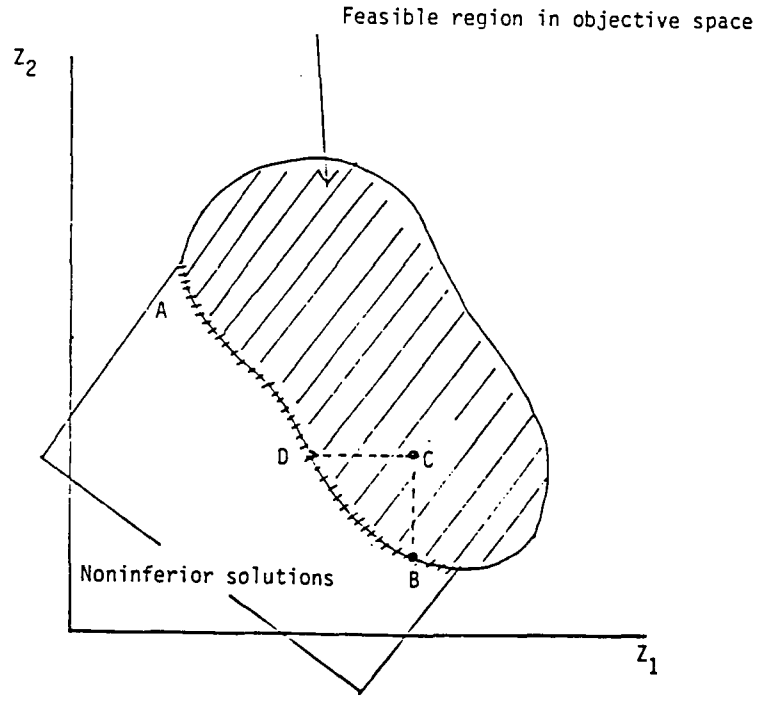


Figure A.4 Graphical interpretation of noninferiority for an arbitrary feasible region in objective space. Lower values of Z_1, Z_2 are preferred to higher values.

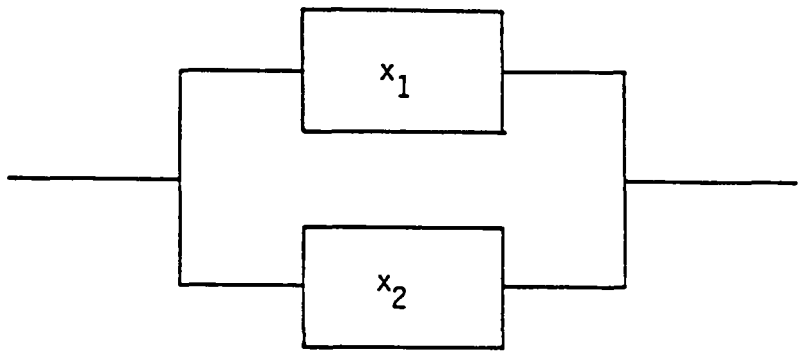


Figure A.5 System configuration for Example 1.

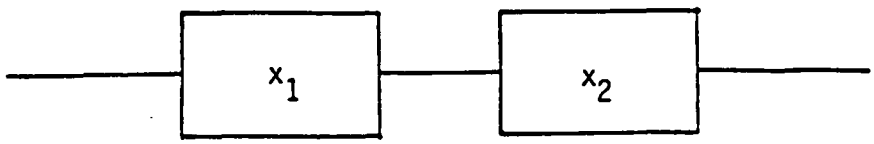


Figure A.6 System configuration for Example 2.

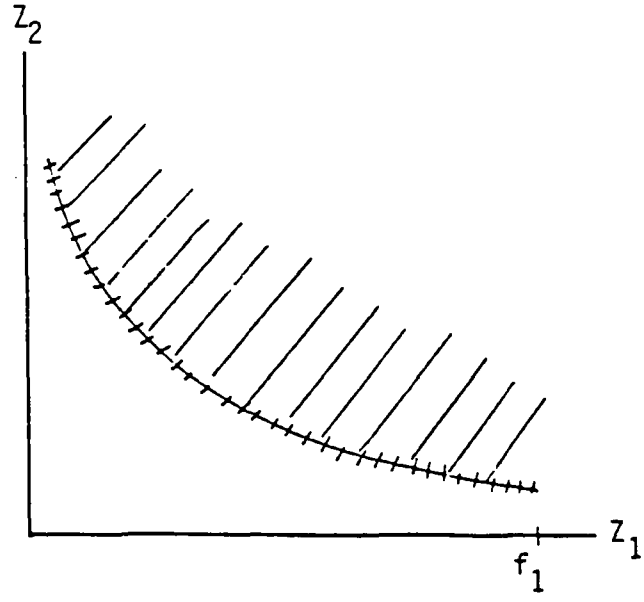


Figure A.7 Noninferior solutions in objective space for Example 1.

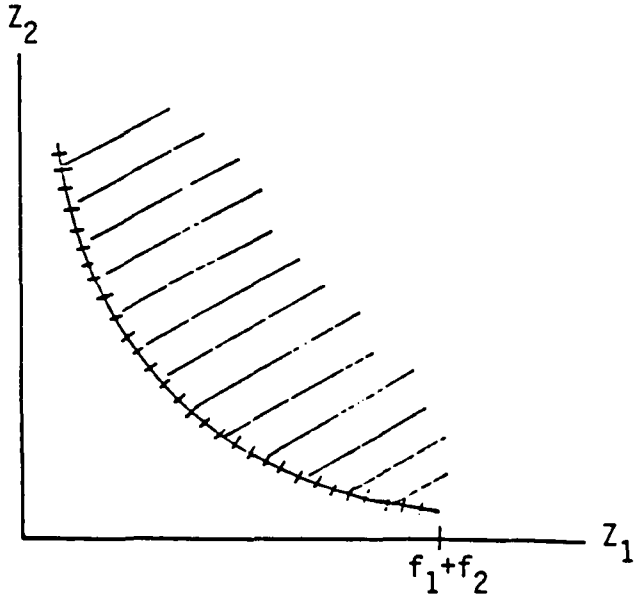


Figure A.8 Noninferior solutions in objective space for Example 2.

APPENDIX B

METHODOLOGY APPLICATIONS

In this appendix we describe applications of the methodology to a more complex PRA model than the example problems presented in Section A.3.3.4. The model was taken from the review[4] of LGS-PRA.[5] Although the PRA model used in this section is not a detailed, full-blown model, it represents a good approximation to a complete PRA model and contains most of the aspects that would be of interest in a demonstration of the proposed methodology. We caution however that the model analyzed here does not and is not intended to represent the Limerick plant. Thus no conclusions should be directly drawn with regard to the safety or operation of that specific plant.

In the first allocation model, we consider as decision variables only the supercomponent unavailabilities in the plant damage matrix. This base model is then extended to include a seismic sequence and also to include containment performance parameters in the decision variables. This extended model demonstrates feasibility of incorporating external events and containment performance within the allocation methodology. Several sensitivity studies with regard to the parameters in the various models and with regard to the PRA model are also included.

B.1 LGS-PRA Review Model

The PRA model can be expressed concisely in matrix formalism (see Section A.3.1):

$$C_d = \underline{f}\ \underline{M}\ \underline{u} \qquad (A.15)$$

$$A = \underline{f}\ \underline{M}\ \underline{C}\ \underline{S}(\underline{a})\ \underline{a} \qquad (A.16)$$

$$L = \underline{f}\ \underline{M}\ \underline{C}\ \underline{S}(\underline{\ell})\ \underline{\ell} \qquad (A.17)$$

where the elements m_{ij} of matrix $\underline{M}$ are functions of "component" unavailabilities x_i's. The effects of maintenance and operator's actions and inactions are also manifested in x_i's or in additional x_i's. The "components" here need to be resolved only to the level at which dependencies of the frontline systems on the support systems are explicitly defined in the matrix M. Thus, it is more appropriate to consider the x_i's as unavailabilities of the "supercomponents".

B.1.1 Internal and Seismic Initiators

We first consider three accident initiators which are the most dominant contributors to core damage and health consequences, i.e., (1) Loss of feed water/main steam isolation valve closure (LOFW/MSIV Closure), (2) Loss of offsite power (LOSP), and (3) Turbine trip (TT). Table B.1 shows the initiator frequencies.

The m_{ij} of the plant damage matrix $\underline{M}$ are as the following:

$$m_{11} = \bar{C}UX + \bar{C}UV$$

$$m_{21} = \bar{C}UX + \bar{C}UV$$

$$m_{31} = \bar{C}QUX + \bar{C}QUV$$

$$m_{12} = \bar{C}\bar{U}W$$

$$m_{22} = \bar{C}\bar{U}W$$

$$m_{32} = \bar{C}Q\bar{U}W$$

$$m_{13} = C\bar{C}'U_H U_R$$

$$m_{23} = C\bar{C}'\bar{U}_H\bar{U}_U\bar{D}W_{12}$$

$$m_{33} = CC'$$

$$m_{14} = C\bar{C}'\bar{U}_R D$$

$$m_{24} = C\bar{C}'\bar{U}_H\bar{U}_R D$$

$$m_{34} = C\bar{C}'\bar{U}_H\bar{U}_R D$$

where indices of m_{ij} stand for

i = 1 LOFW/MSIV Closure
i = 2 LOSP
i = 3 TT
j = 1 Plant Damage State (Accident Class) I
j = 2 Plant Damage State (Accident Class) II
j = 3 Plant Damage State (Accident Class) III
j = 4 Plant Damage State (Accident Class) IV

and Table B.2 defines other notations. Table B.2 also defines safety functions in terms of systems.

Table B.3 lists event descriptions of "components" which are fed into fault trees shown in Figures B.1 through B.9.

Next, we consider the seismic accident initiator. The frequency of plant damage state j=5 due to a seismic event is expressed as

$$f_4 m_{45} = \int_{a_\ell}^{a_u} h(a)\, S_5\,(Y_1(a),\, Y_2(a),\, \ldots,Y_S(a))da$$

where h(a) is the seismic hazard (intensity) function, S_5 the minimal cut set expression of a seismic accident sequence leading to the plant damage state j=5 (a seismic state), a_ℓ and a_u are the lower and upper cutoff peak ground accelerations at the site respectively, and $Y_i(a)$ is the fragility

function for "seismic component" i, usually assumed to be a cumulative standard normal distribution function[18]:

$$Y_i(a) = \Phi\left[\ln \frac{a}{\hat{A}_i} / \beta_i\right]$$

with

$\hat{A}_i$ = "best-estimate" of the median ground acceleration capacity for component i

and

β_i = logarithmic standard deviation associated with the underlying randomness of the capacity.

We consider in the extended allocation model that $\hat{A}_i$ and β_i are the decision variables for seismic component i. A discretized approximation to the expression of $f_4 m_{45}$ is

$$f_4 m_{45} = \sum_{j=1}^{N} [h(a_j)\Delta a_j \; S_5\{(Y_1(a_j), Y_2(a_j), \ldots, Y_s(a_j)\}]$$

The seismic sequence included in the methodology applications is the $T_S R_B$ sequence in Refs. 19 and 20. This sequence represents a seismic initiator failing the reactor enclosure and control structure followed by containment failure. The cumulative hazard curve used in the calculations is shown in Figure B.10.

The site matrices used are taken from Ref. 4 and shown in Table B.6.

B.1.2 Modeling of Containment Performance

The "strength" of the containment was also included as a decision variable through the "probability of containment failure" S. We again caution that the containment model developed here does not represent the Limerick containment, per se. It is simply used to illustrate how decision variables might be included in a containment matrix. No inferences should be drawn from the analysis with regard to the Limerick plant. The containment matrix $\underline{C}$ for the LGS review is given in Table B.7. The parameters in the matrix correspond to the probabilities of various containment failure modes as follows:

α_1: Probability of in-vessel steam explosion x Probability of Reactor Pressure Vessel (RPV) rupture x Probability of Containment failure. This joint probability corresponds to classes I and III. Nominal value in the Limerick review is: $10^{-3} = 10^{-1} \times 10^{-1} \times 10^{-1}$. In this simplified model α_1 was put equal to

$$\alpha_1 = 10^{-2}S \; .$$

That is, the probability of the physical phenomena and the non-containment related failures are kept constant. If $S = 10^{-1}$ we get the nominal Limerick case. For $S > 10^{-1}$ we get weaker than Limerick containment while for $S < 10^{-1}$ stronger.

α_2: Probability of in-vessel steam explosion x Probability of RPV rupture in an already failed containment. This joint probability corresponds to classes II and IV. Nominal value for the Limerick review is 10^{-2}. Since this probability does not depend on the containment strength (it has already failed) it should be kept constant as the strength of the containment changes. Since, however, a stronger than the nominal case containment will fail later and a weaker sooner, there would be a corresponding effect on the available warning time. A longer or shorter warning time would result on higher or lower consequences than the nominal case. Since the site matrix does not change, this effect is included by setting

$$\alpha_2 = 10^{-1} S .$$

If $S = 10^{-1}$ we get the nominal case, i.e., the Limerick containment. If $S > 10^{-1}$ or $S < 10^{-1}$, we get weaker or stronger than Limerick containment.

β_1: Probability of ex-vessel steam explosion x Probability of Containment failure. This joint probability corresponds to classes I and III. In the simplified model it was set $\beta_1 = 10^{-1}S$. If $S = 10^{-1}$ we get $\beta_1 = 10^{-2}$ the nominal case for Limerick containment.

β_2: Probability of ex-vessel steam explosion in an already failed containment. This probability corresponds to classes II and IV. For reasons similar to those for the in-vessel steam explosion we set $\beta_2 = S$. If $S = 10^{-1}$ we get $\beta_2 = 10^{-1}$ the nominal case for Limerick containment. For $S > 10^{-1}$ and $S < 10^{-1}$ we get weaker and stronger than Limerick containment, respectively.

μ': Probability of Hydrogen Detonation. It is assumed that it does not depend on the strength of the containment.

γ: Conditional probability of containment failing in the dry-well given it fails from overpressure. Limerick nominal case is $\gamma = 0.50$.

γ': Conditional probability of containment failing in the wet-well above the suppression pool surface, given that the containment fails from overpressure. Limerick nominal case is $\gamma' = 0.25$.

γ'': Conditional probability of containment failing in the wet-well below the suppression pool surface given that the containment fails from overpressure. Limerick nominal case is $\gamma'' = 0.25$.

The simplified model keeps the relative failure likelihoods of the points constant (i.e., 0.50:0.25:0.25) and uses the variable S to describe the strength of the containment. Thus,

$$\gamma = 5 \times S, \quad \gamma' = 2.5 \times S, \quad \gamma'' = 2.5 \times S.$$

If $S = 10^{-1}$ we get the Limerick nominal case, for $S > 10^{-1}$ and $S < 10^{-1}$ we get weaker and stronger containment, respectively.

B.2 Reliability Cost Functions

The nominal component reliability cost functions used in the methodology applications are for all components

$$g_i(x_i) = a_i(1/x_i - 1) + b_i \ .$$

The parameters a_i and b_i are shown in Table B.4. The choice of the functional form and the parameters here is only for illustration purposes, and in a real problem they are to be determined by field cost data. In Section B.3.3, a tabular form of cost information is used to incorporate in the cost model the feature of reliability improvement by redundancy. It is noted that the unit of the reliability costs needs not be specified at this stage of the methodology (i.e., determination of the noninferior solutions), as long as all the reliability costs are expressed in a common unit, for example, in dollars ($). The unit should, however, be specified at the stage of preference assessment.

Table B.5 shows the upper and lower limits of component unavailabilities considered in these applications. It is noted that the lower limits could be interpreted as technological constraints or other physical feasibility limitations in improving the component reliability. Table B.5 also includes for convenience of reference the nominal unavailabilities of the Limerick PRA review.

B.3 Results and Discussions

In order to demonstrate the methodology, a series of calculations were performed using the PRA model and reliability cost functions presented in Sections B.1 and B.2. The results are grouped into three sets of calculations according to the extent of the model parameters treated as decision variables. The first set of calculations represents the results of the base model in which only the supercomponent unavailabilities in the plant damage matrix $\underline{M}$ are the decision variables (see Section B.1). The values used for initiator frequencies, containment and site matrices were the best-estimates in Ref. 4 and are reproduced in Tables B.1 and B.6. The second set of calculations is the results for the extended model which includes, in the set of decision variables, the containment failure probability and a seismic sequence. The third set of results consists of several sensitivity calculations on the cost models and on the site matrix.

B.3.1 Base Model

The results of the base model were presented with discussions in Section 3 of the Main Report and are not repeated here.

B.3.2 Extended Model

The results of the extended model are presented in Tables B.8 through B.10 and in Figures B.11 and B.12.

As in the base model, the set of noninferior solutions represents a hypersurface in the four-dimensional space (C_d, A, L, G). The intersections of this surface with a hyperplane corresponding to a constant value of C_d [i.e., (C_d = const, A, L, G)] is a curve in the three-dimensional space (A, L, G). The "projection" of this curve on the (A, G) plane gives a trace which is depicted in Figure B.11 for several values of C_d. Figure 4.12, on the other hand, depicts the projection of the (C_d = const, A, L, G) curves on the (L, G) plane.

Examination of these traces leads to similar general observations as for the base model (see Section 3.1).

i) Each trace, for example on the (A, G) plane, Figure B.11, is characterized by two extreme points (lower and upper limits). For the C_d = 10^{-4}/reactor year case, for example, these two extreme points are points C_1 and C_5. Point C_1 means that it is not efficient to lower the unavailabilities of the systems or increase the strength of the containment, keeping the core damage frequency constant at 10^{-4}/ry in order to decrease acute fatalities. If we do so we will get a solution that will be inferior to another that will have the same acute fatalities, the same or lower latent fatalities, the same or lower cost, but lower core damage frequency. At the other end, point C_5 means that it is not possible to increase the acute fatalities further by increasing system unavailabilities or decreasing containment strength (and hence lowering cost) and at the same time keep the core damage frequency constant at 10^{-4}/ry. The value of the variable X(22), representing the failure probability of the containment, S, that corresponds to point C_5 is equal to unity. In other words, this solution corresponds to a design "almost without" containment.

ii) As in the case of the base model, the acute and latent fatalities vary in the same direction. That is, an increase in acute fatalities is always associated with an increase in latent fatalities (for constant core damage frequency). Again as in the base model the relative change of the acute fatalities is larger than that of the latent fatalities. This behavior is due to the greater correlation that exists between core damage frequency and latent fatalities. In other words, it is easier to change the acute fatalities while keeping the core damage frequency constant than it is to change the latent fatalities.

iii) The range of possible values for acute and latent fatalities at constant core damage frequency is larger in the extended model than in the base model (compare Figures 3.1 with B.11 or Figures 3.2 with B.12). This is due to the additional flexibility that is provided by the inclusion of the containment failure probability as a decision variable.

iv) The variation from the lower values to the higher values of each trace for acute fatalities is due practically to the variations of the containment strength [X(22)] and the unavailability of the Reactor Protection System [X(1)]. All the other system unavailabilities remain practically constant (for constant core damage frequency). For example, starting from the solution yielding the highest acute

fatalities (e.g., D_5 for $C_d = 5 \times 10^{-5}$/ry) we observe that the containment failure probability, X(22), has its highest possible value (almost no containment), while the RPS unavailability, X(1), has the maximum value allowed by the constraint of $C_d = 5 \times 10^{-5}$/ry and the minimization of the total cost (see Table B.10). Lower acute fatalities and higher cost solutions are achieved by lowering the values X(1) and X(22) in such a way that their combined cost remains minimum. Starting from D_5 and moving towards D_1, X(1) and X(22) vary at about the same rate up to D_2. After that, X(22) changes faster than X(1). The effect of a decrease in X(1) on the frequency of core damage is offset by an appropriate increase of the Standby Liquid Control System unavailability, X(2).

v) It is noteworthy that for $C_d = 10^{-3}$/ry (Figure B.11 or Table B.8) the noninferior solutions indicate a value for X(22) equal to unity. This containment failure probability is equivalent to almost no containment. This means that starting with the solution A_5, it is more cost-effective to decrease acute fatalities by decreasing the unavailability of the Reactor Protection System [X(1)] rather than enhancing the strength of the containment. This is true up to point A_1. If we want to decrease acute fatalities further, it is more cost-effective to do so by decreasing unavailabilities of the other appropriate systems (these also result in reduced core damage frequencies) rather than improving the containment. All of these results are of course subject to the validity of the assumed cost functions.

vi) As we move from right to left on each trace, for example from A_5 to A_1 in Figure B.11, the median ground acceleration capacity of the re actor building, X(20), increases (see Tables B.8-B.10). The rate of increase becomes larger as the core damage frequency decreases. Thus for $C_d = 10^{-4}$/ry the capacity increases so fast that at point C_4 it already becomes 1.50g which is the assumed technological upper limit of the capacity, whereas for $C_d = 10^{-3}$/ry it varies from 0.93g to 1.30g. The reason is the following. The relative contribution to the core damage frequency of the seismic sequence $T_S R_B$ (accident class V) in comparison with other accident classes, e.g., accident class I which dominates the core damage frequency, increases as the core damage frequency decreases. The seismic sequence is, however, the most dominant contributor to the acute fatalities given occurrence of the initiator (see the site matrix, Table B.6). Thus, as the core damage frequency decreases X(20) becomes "felt" as the contributor to the core damage frequency and it becomes more cost-effective to increase the capacity early. However, at a higher core damage frequency, e.g., $C_d = 10^{-3}$/ry the relative contribution of the seismic sequence to the core damage frequency becomes so small that X(20) is now controlled more by the acute fatalities. At this high core damage frequency, the contribution of the seismic sequence to the acute fatalities is, however, overshadowed by other accident classes so that X(20) is now allowed to have lower capacities.

A step by step informal preference assessment by screening out less preferred options (see Sections 2.6 and 3.1) leads to the same general conclusions about the range of unavailability of the various decision variables as in the case of the base model.

B.3.3 Sensitivity Analyses

B.3.3.1 Parameter Sensitivity Analysis

An extended model was used to examine the sensitivity of the results to the several cost models and to the site matrix. A different containment model than the one considered in Section B.1.2 was used. This containment model includes, in the set of decision variables, the conditional probabilities of release categories given a specific accident class (plant damage state). These are defined in Tables B.11 and B.7. Tables B.12 through B.15 describe the various cost models. Figure B.13 depicts the reliability cost function contained in Table B.15 and represents a reliability cost behavior for the diesel generator system which would be characterized not only by improving reliabilities of diesel generators in a fixed configuration but also by increasing the redundancy of the diesel generator system. The configuration changes from a single diesel generator system (point 1 in Figure B.13) to a two diesel generator system (point 2 in Figure B.13) by adding a diesel generator of same reliability (and so of same cost) at point 1. Note that the cost at point 2 is twice that of the cost at point 1 (log-log scales in Figure B.13). The two points are then smoothly interpolated to avoid numerical difficulties. Table B.6 provides the lower-, upper-, and best-estimates for the site matrix.

The results of sensitivity calculations are provided in Figures B.14 through B.17 and in Tables B.17 and B.18. The calculations were performed only for a core damage frequency of 1×10^{-4}/ry. Qualitatively, the three general observations noted in Section B.3.2 are also applicable here. In addition to the general observations, several noticeable features of the results are as follows:

i) The reliability cost models in Table B.13 and B.14 tend to extend the lower limits of the noninferior solution traces with corresponding variations of the reliability cost (SC- and CC-traces in Figures B.14 and B.15). The extension of the lower limits of the acute fatalities is quite substantial.

ii) The reliability cost model in Figure B.13 and Table B.15 (tabular form to reflect a redundant configuration of the diesel generator system) tends to lower the reliability cost curve but not change the extreme points of the noninferior solution traces (RC-traces in Figures B.14 and B.15).

iii) The lower-estimate in the site matrix tends to lower the reliability cost at the lower limits of the traces but not at the upper limits of the traces (LC-traces) in Figures B.16 and B.17).

iv) The upper-estimate in the site matrix tends to shrink the lower limits of the traces. It tends to increase the reliability cost at the lower limits of the traces but not at the higher limits of the traces (UC-traces in Figures B.16 and B.17).

As can be seen from Tables B.17 and B.18, the unavailabilities of many components, e.g., X(4), X(5), X(6), and so on, are insensitive to the assumptions of the cost models and the site matrix for the whole range of the

traces. As we move toward the upper limits of the traces, all components except the diesel generator system [X(16)] become more insensitive. As we move, however, toward the lower limits of the traces, some components, e.g., X(1), X(2), X(11), X(12), and X(22) through X(29) become quite sensitive. These observations imply that the degree of sensitivity of the allocated unavailabilities depends upon where our interests lie in the region of the noninferior solution set. This in turn depends on the decision maker's preferences. In other words, if the preference assessment of the decision maker leads toward the lower limits of the traces, the corresponding unavailabilities would be less well-established and uncertainty analyses would be desired, while if the preference assessment leads toward the upper limits of the traces, the corresponding unavailabilities would be well-defined and uncertainty analyses may not be warranted. Conversely, sensitivity studies such as those described above or simple uncertainty analyses as described in Appendix D would help the decision maker articulate his preferences toward the region of less sensitivity or more certitude (toward the region of upper limits of the traces in our example problem).

B.3.3.2 PRA Model Sensitivity Analysis

The base model in Section 3 of the main report was used as the reference model to examine the sensitivity of the allocation results to the PRA model. The PRA model of a plant usually consists only of dominant accident sequences remained after truncation processes. Thus, it would be worthwhile to see how the allocation results are affected by the truncation of the PRA model. Two cases are examined for this purpose.

Case 1 includes in the PRA model a large LOCA initiator, in addition to the three dominant accident initiators, i.e., (1) loss of feedwater/main steam isolation valve closure (LOFW/MSIV Closure), (2) loss of offsite power (LOSP), and (3) turbine trip (TT), considered in the base model. Inclusion of the large LOCA adds four additional accident sequences to the set of 15 accident sequences in the base model. The total number of basic events remains, however, the same 19 supercomponents as in the base model. The additional m_{ij} of the plant damage matrix $\underline{M}$ are as follows:

$$m_{41} = m_{42} = 0$$

$$m_{43} = \text{RHRH} + (\text{EDC})(\text{RECOV})$$

$$m_{44} = C$$

where Table B.2 defines the notations. The initiator frequency for the large LOCA is 4×10^{-4}/ry from Reference 4.

Case 2 includes in the PRA model an initiator of inadvertent opening of safety-relief valves (IORV), in addition to the three dominant initiators in the base model. Inclusion of this IORV adds seven additional accident sequences. The total number of basic events also increases from 19 to 24 supercomponents which are shown in Table B.19. The additional m_{ij} of the plant damage matrix $\underline{M}$ are as the following:

$$m_{41} = m_{42} = 0$$

$$m_{43} = C_E KPU + C_E KC' + CPU + CC'$$

$$m_{44} = C_E KC'' + CC'' + C_E KM + CM$$

where the notations are defined in Tables B.2 and B.19. The initiator frequency for the IORV is 0.25/ry from Reference 4.

The results of model sensitivity calculations are provided in Tables B.20 through B.24 and in Figures B.18 through B.20. The calculations were performed only for the upper limits. The noninterior solutions for Case 1 are represented as A6', B5', C8', and D8', and the noninterior solutions for Case 2 as A6", B5", C8", and D8". The corresponding noninferior solutions for the base model are represented as A6, B5, C8, and D8. Table B.24 provides the ranges of unavailabilities suggested by the noninferior solutions remained after a preliminary screening process described in Section 3.1. The ranges of unavailabilities for some of the supercomponents are plotted in Figure B.20 as aspiration levels or target bands, and are compared with the model plant nominal unavailabilities.

It is observed that both the global measures and the lower level unavailabilities are insensitive to the difference of the three PRA models used in this sensitivity analysis. Although the sensitivity results tend to deviate more as we move toward a larger core damage frequency, the deviation at the core damage frequency 1×10^{-3}/ry are still considered very small. This indicates that the allocation results would not be affected significantly by the truncation inherent in the PRA model if the PRA model used represents the plant reasonably well.

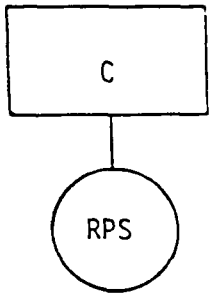


Figure B.1 Functional fault tree for reactor protection.

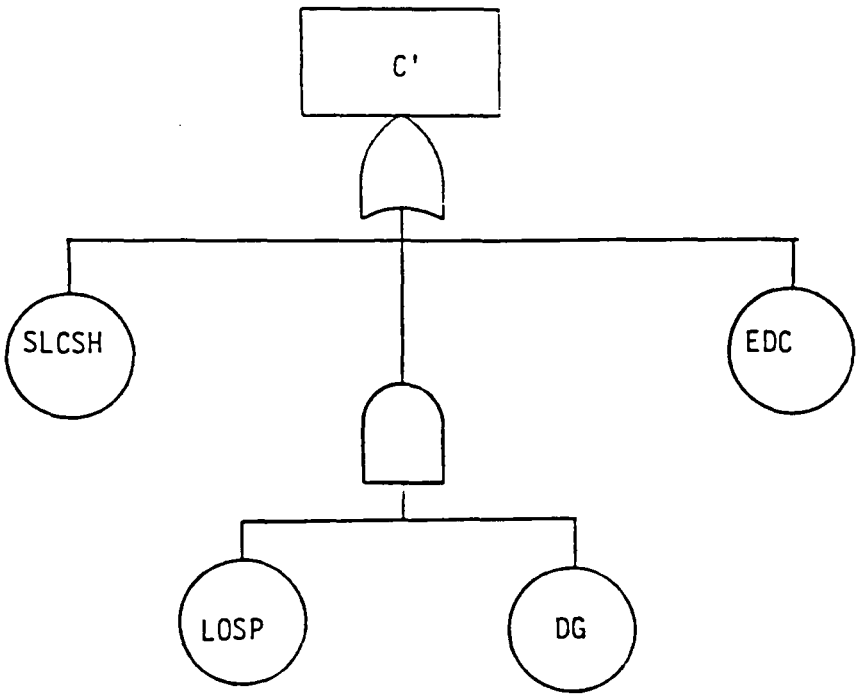


Figure B.2 Functional fault tree for poison injection.

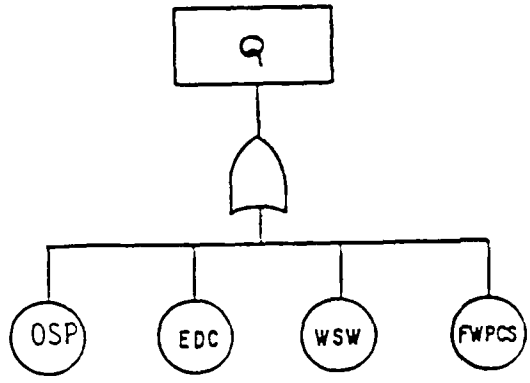


Figure B.3 Functional fault tree for feedwater injection function.

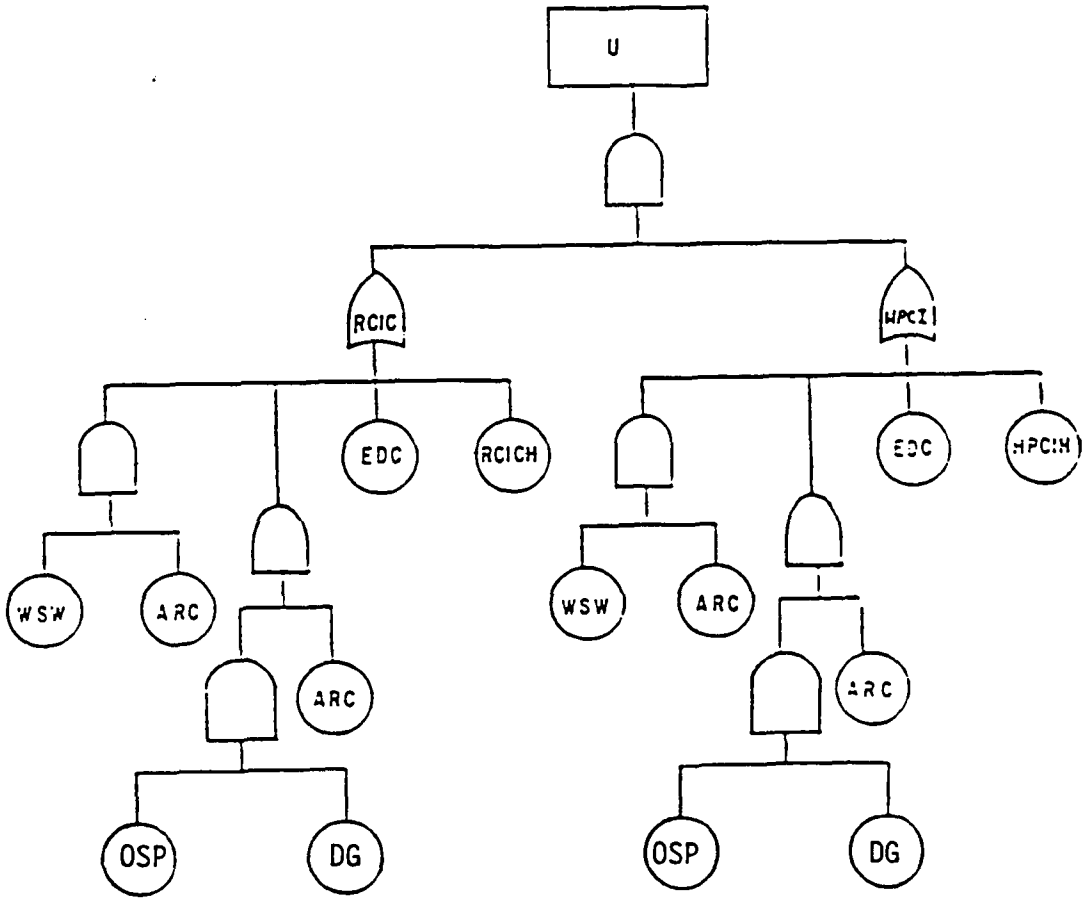


Figure B.4 Functional fault tree for high pressure injection function.

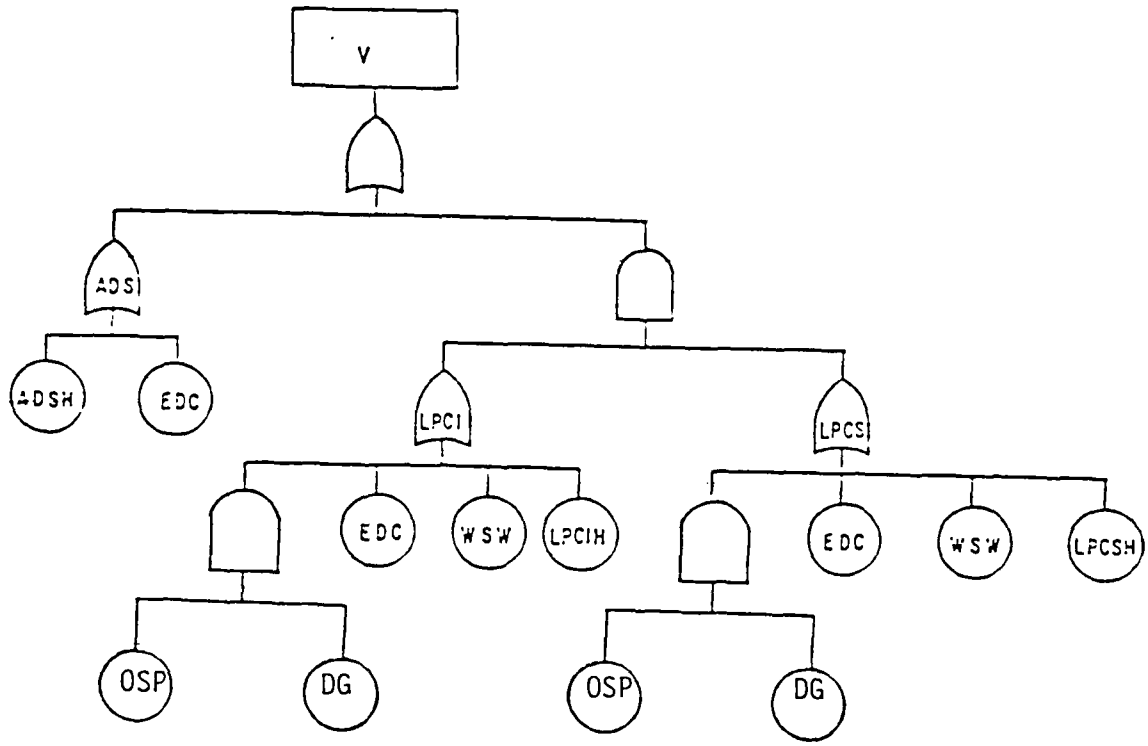


Figure B.5 Functional fault tree for low pressure injection function.

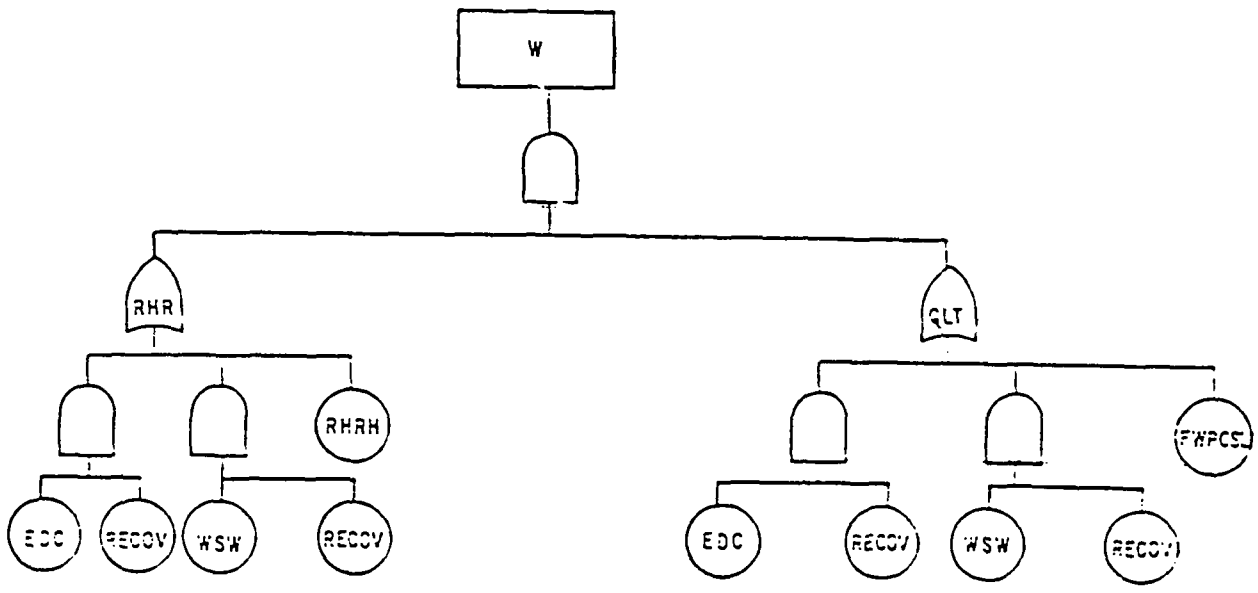


Figure B.6 Functional fault tree for containment heat removal function.

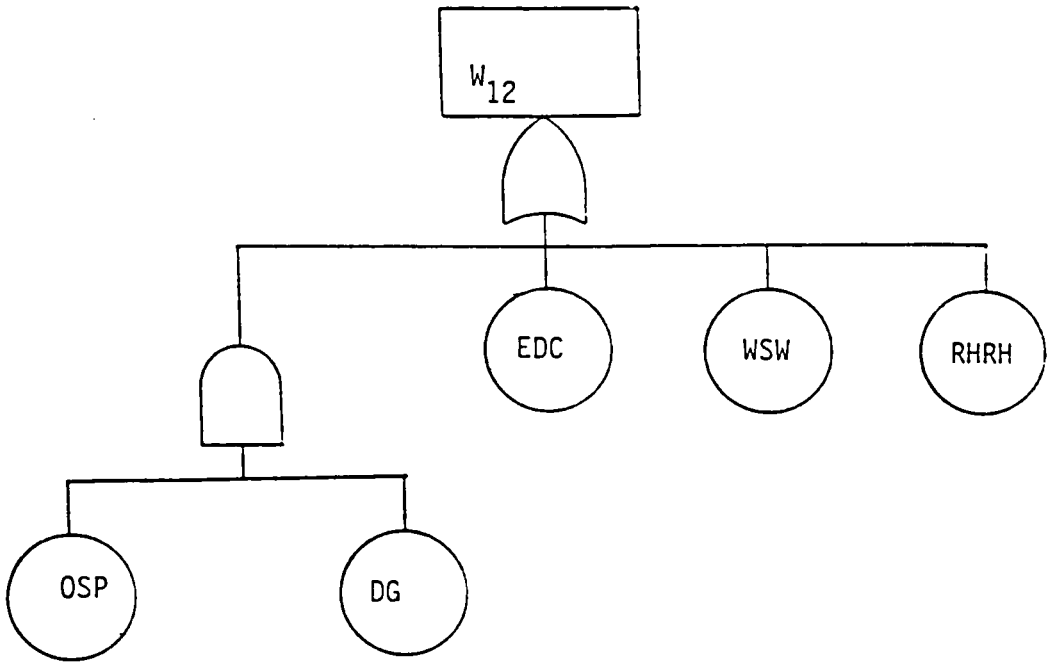


Figure B.7 Functional fault tree for containment heat removal function (short-term).

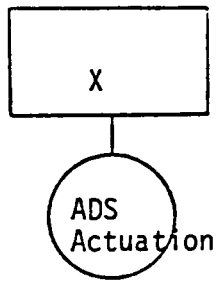


Figure B.8 Functional fault tree for ADS depressurization.

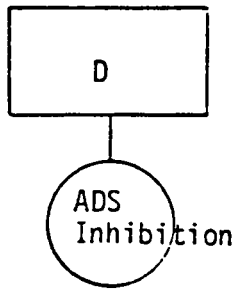


Figure B.9 Functional fault tree for ADS inhibition.

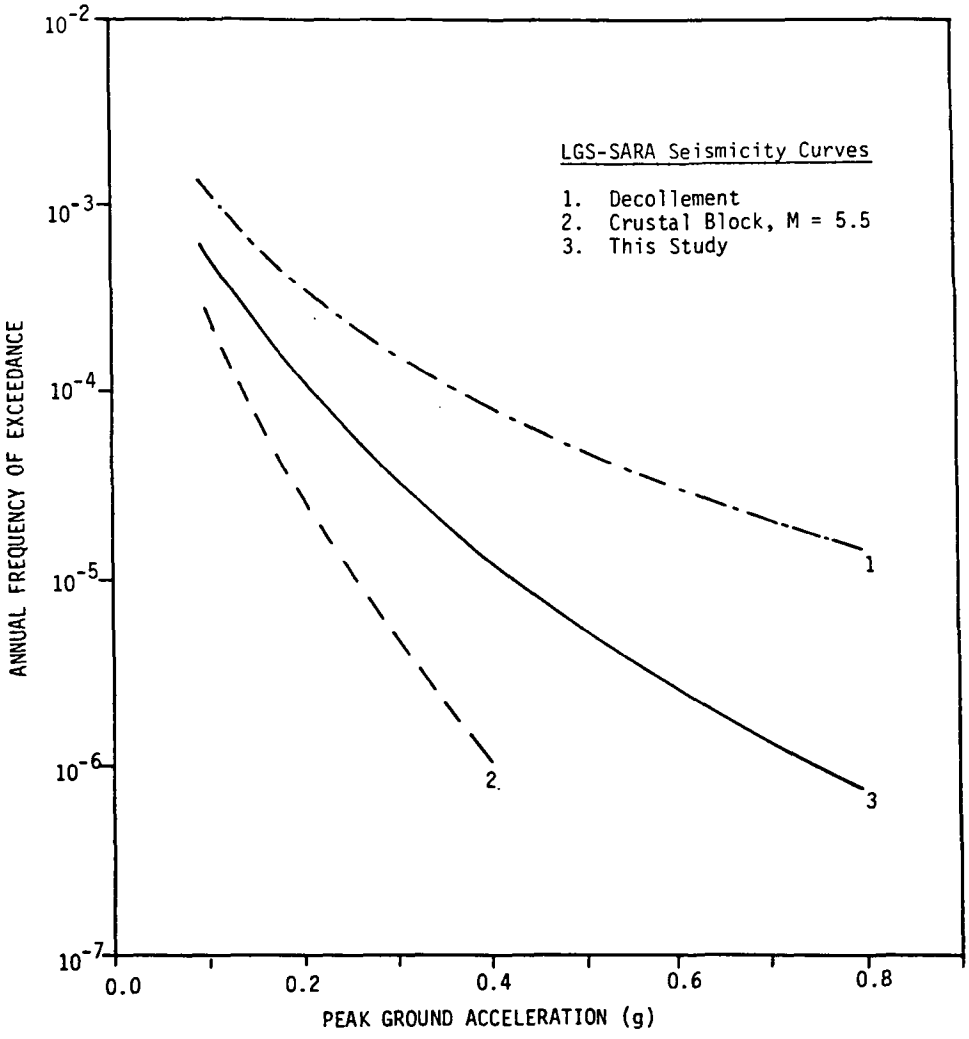


Figure B.10 Seismicity curve for sustained-based peak ground acceleration.

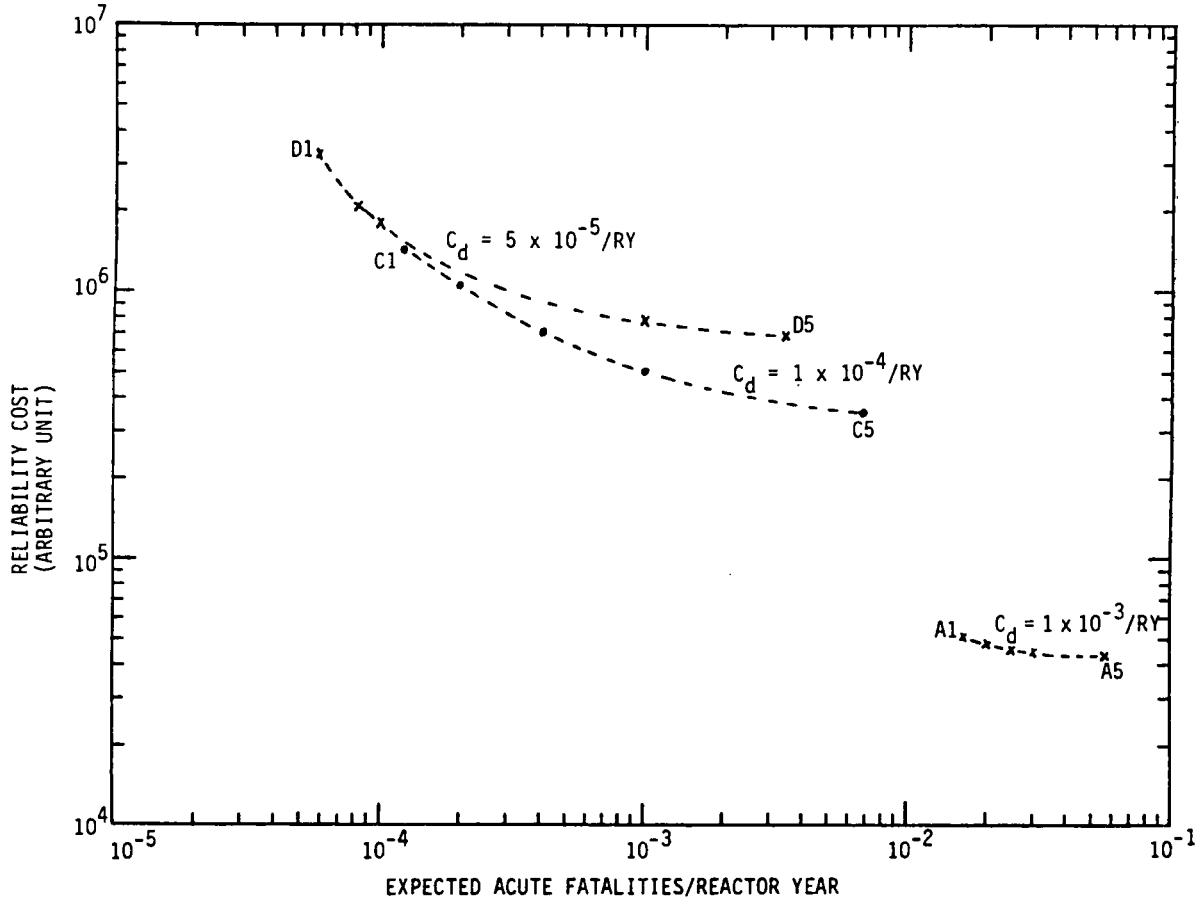


Figure B.11 A two-dimensional display of noninferior outcomes at several core damage frequencies for the extended model.

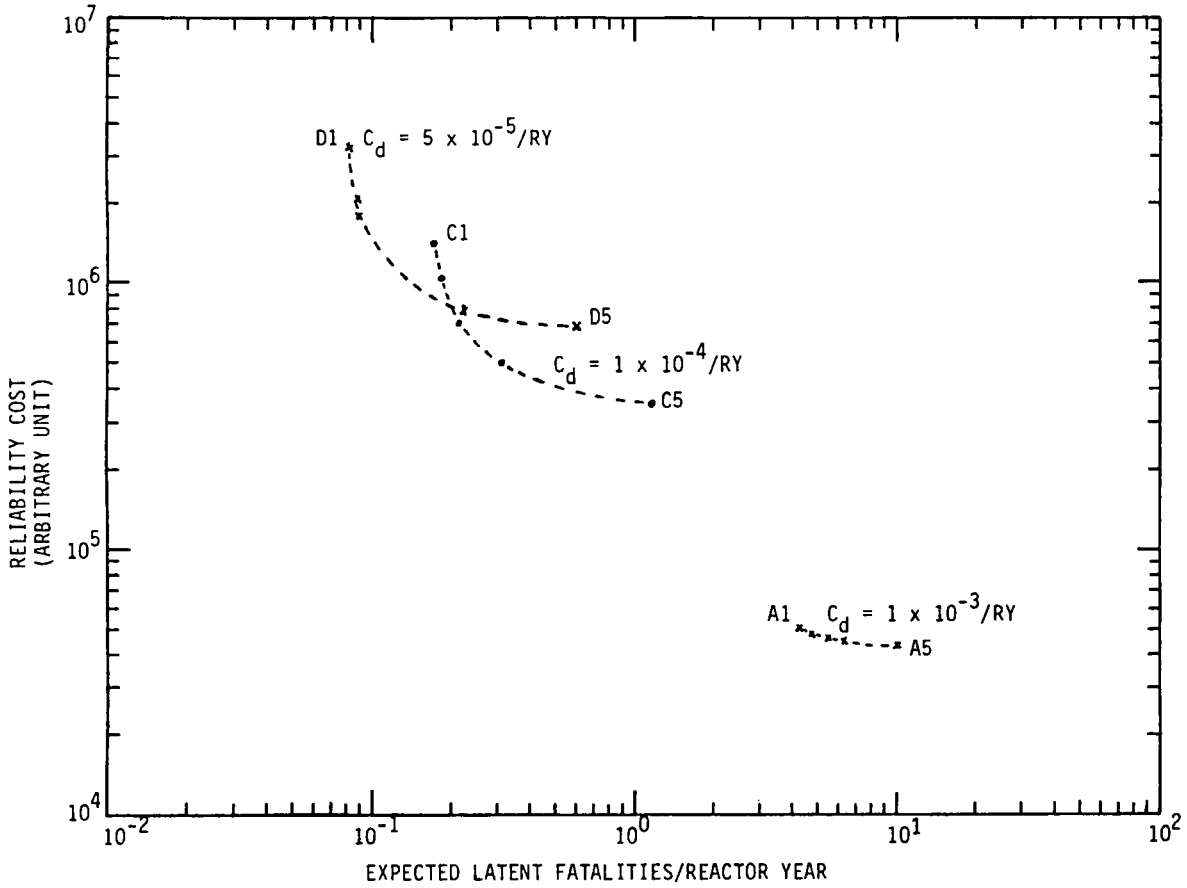


Figure B.12 A two-dimensional display of noninferior outcomes at several core damage frequencies for the extended model.

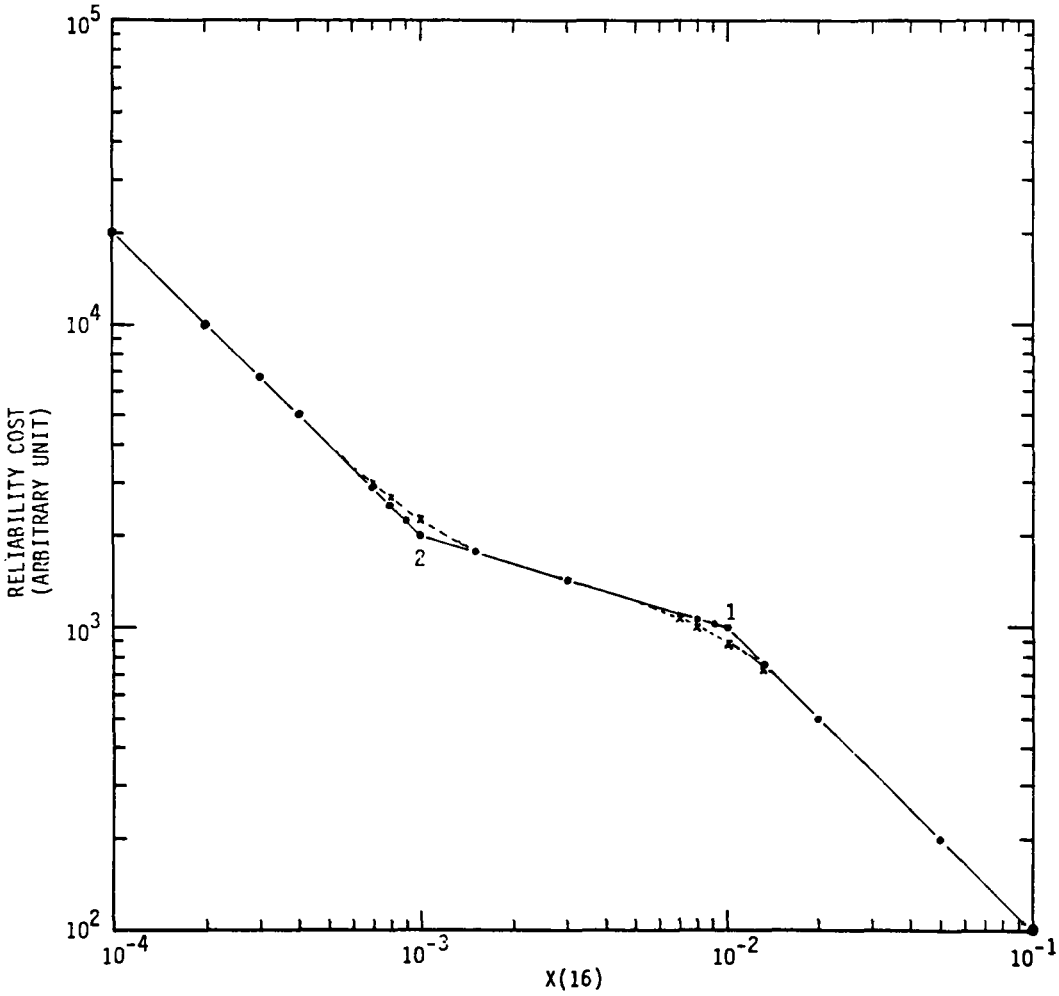


Figure B.13 A reliability cost function for the diesel generator system with redundancy.

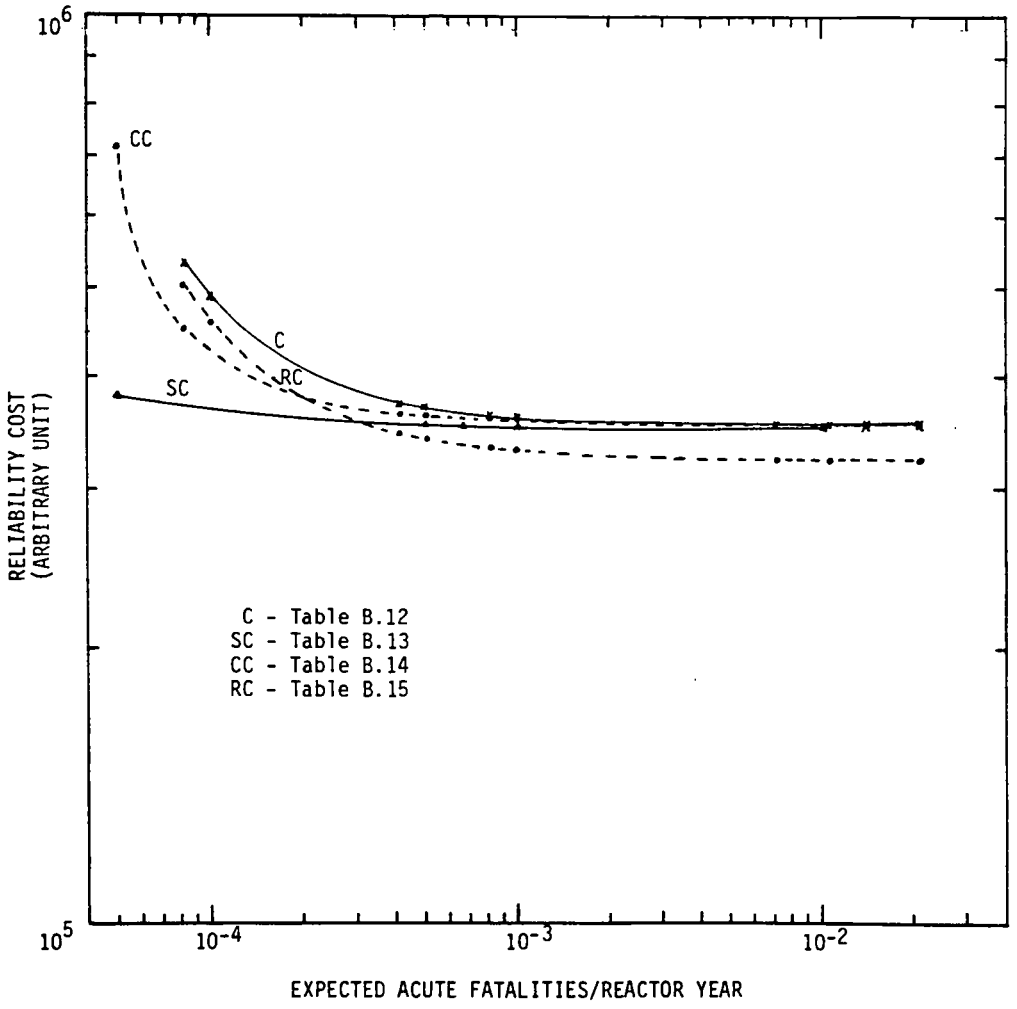


Figure B.14 A two-dimensional display of noninferior outcomes using several cost models at $C_d = 1 \times 10^{-4}$/ry.

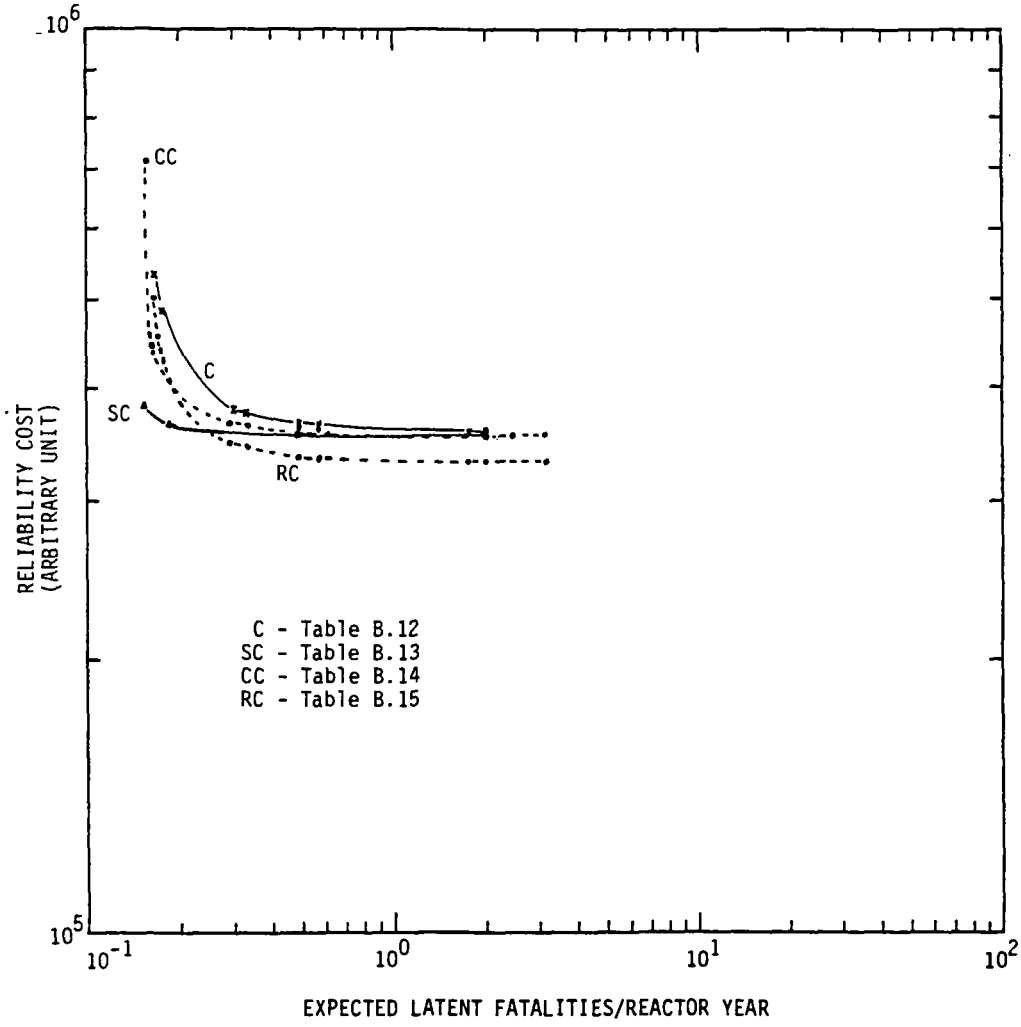


Figure B.15 A two-dimensional display of noninferior outcomes using several cost models at C_d = 1 x 10^{-4}/ry.

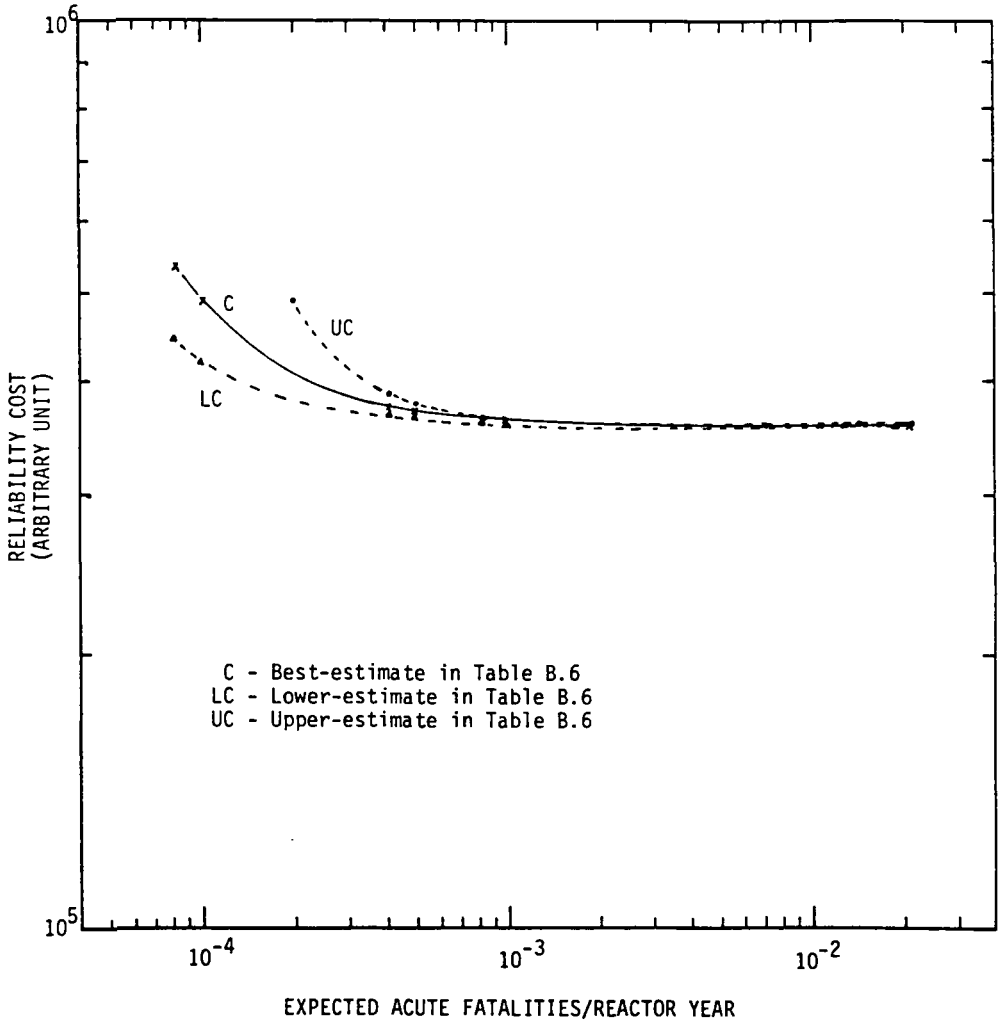


Figure B.16 A two-dimensional display of noninferior outcomes using several site matrices at $C_d = 1 \times 10^{-4}$/ry.

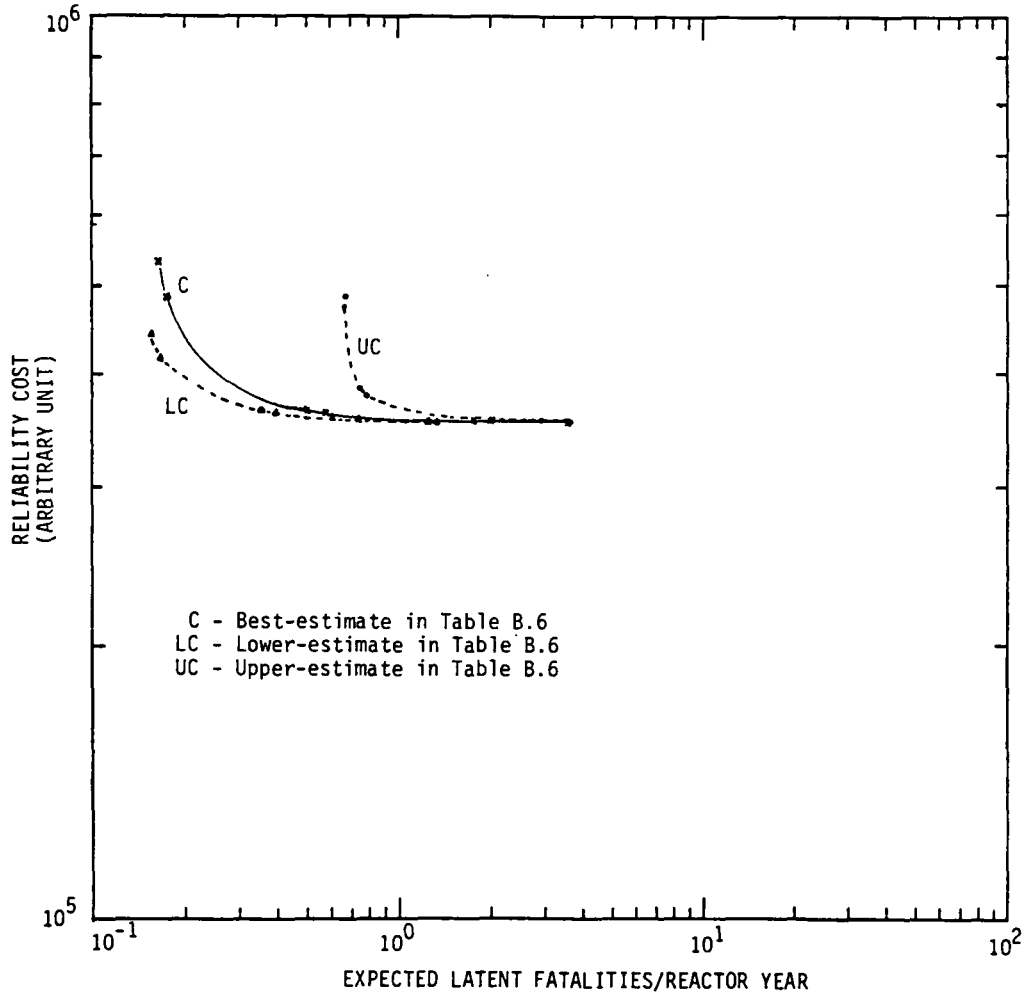


Figure B.17 A two-dimensional display of noninferior outcomes using several site matrices at $C_d = 1 \times 10^{-4}$/ry.

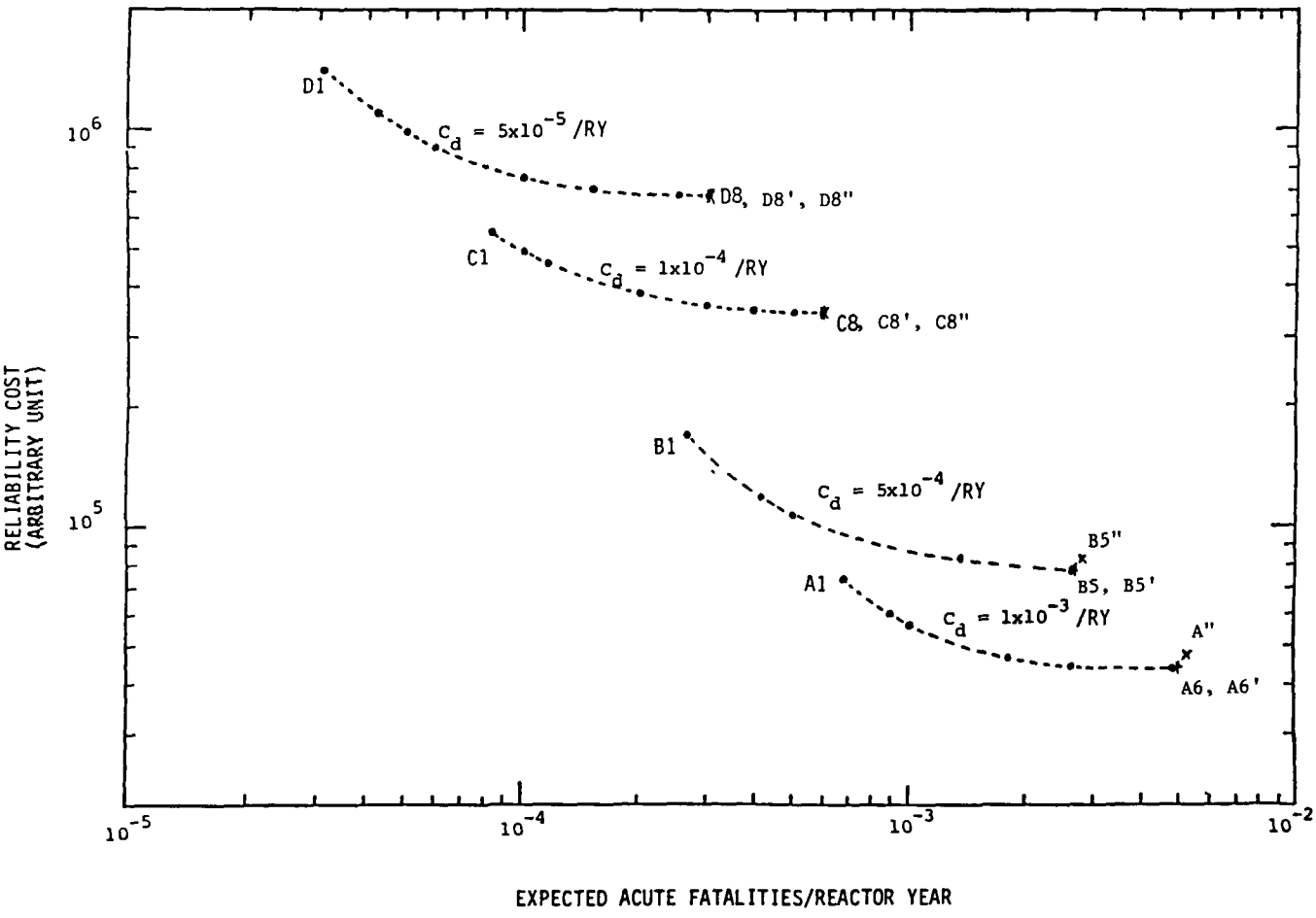


Figure B.18 A two-dimensional display of noninferior outcomes at several core damage frequencies; two sensitivity models compared with the base model.

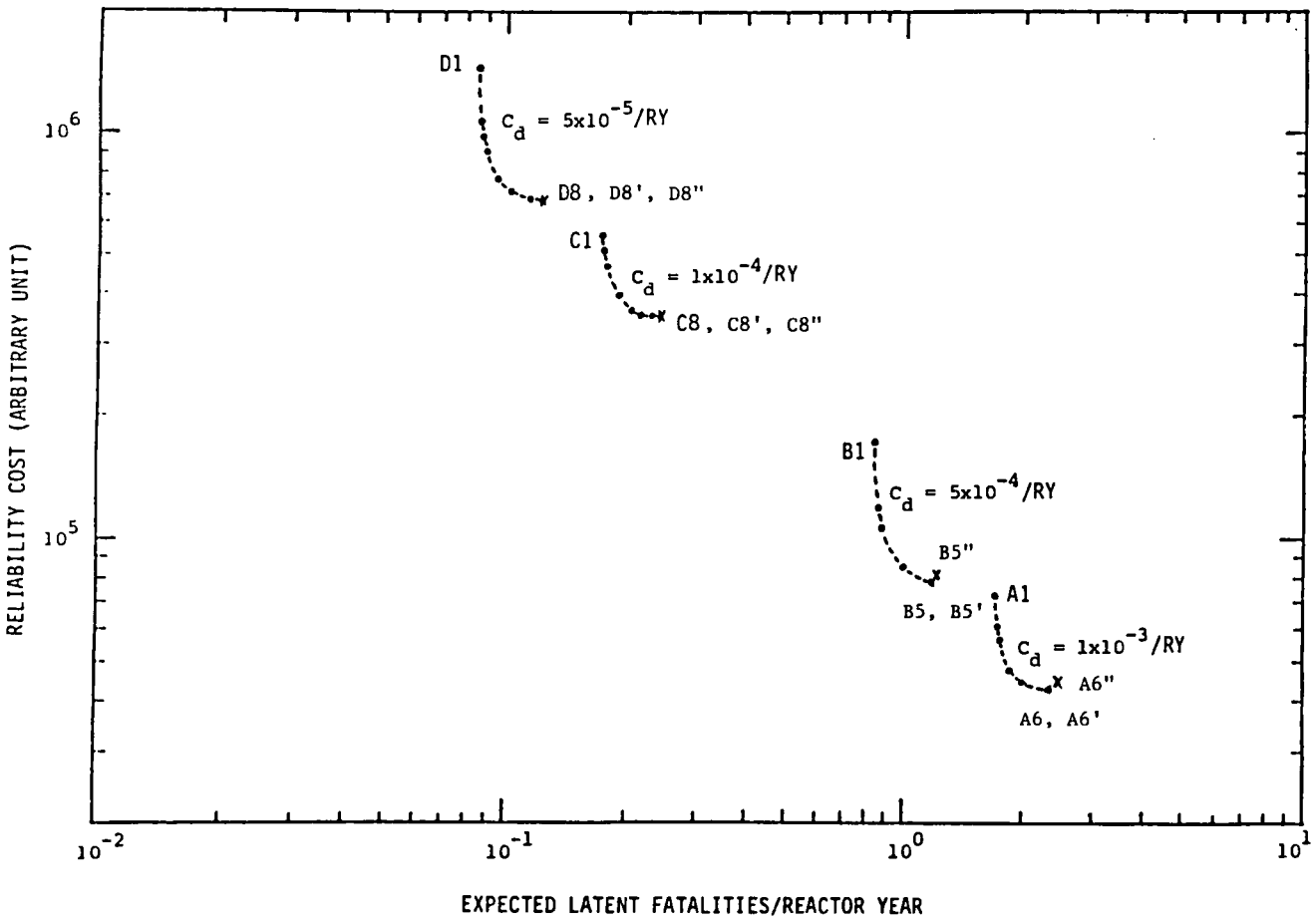


Figure B.19 A two-dimensional display of noninferior outcomes at several core damage frequencies; two sensitivity models compared with the base model.

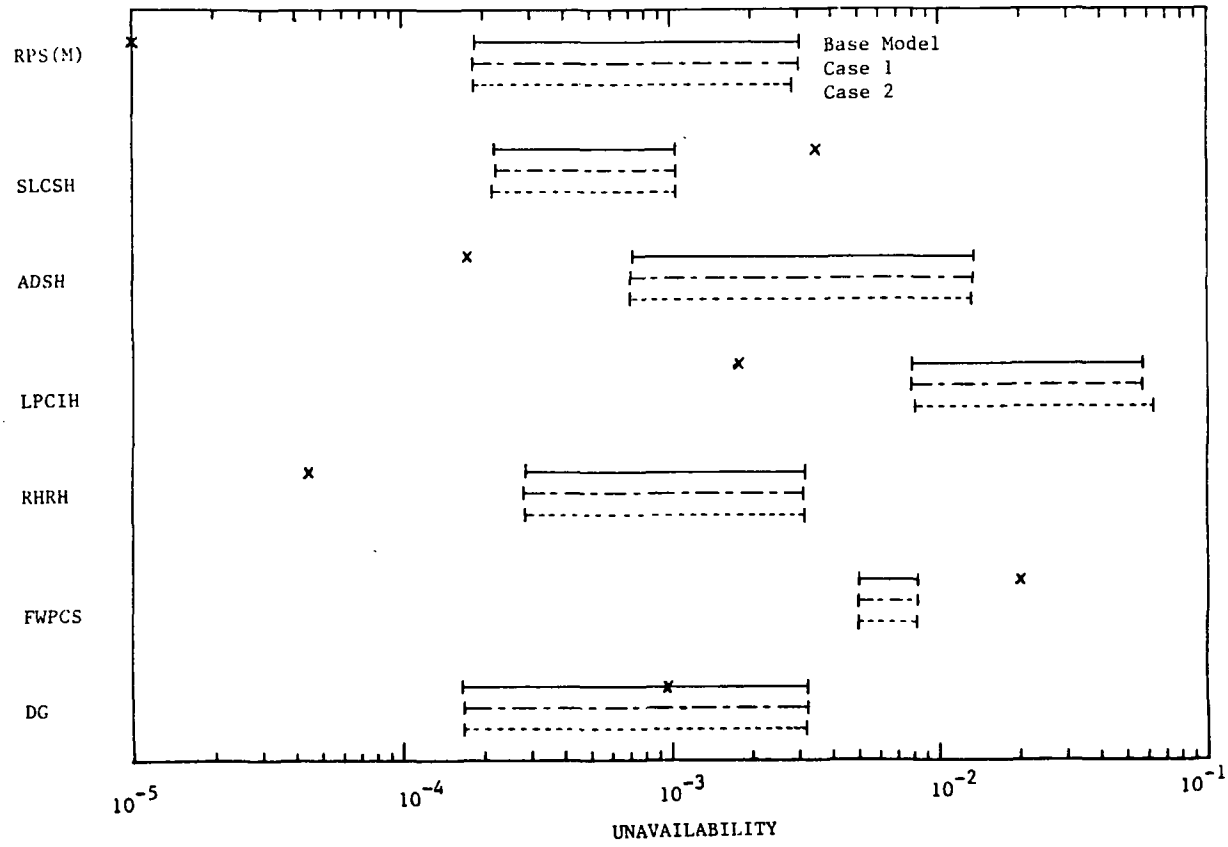


Figure B.20 Aspiration levels (target bands) obtained from base model and sensitivity models in comparison with model plant nominal unavailabilities (X).

Table B.1 Initiator Frequency

Initiator	Events/Reactor Year
LOFW/MSIV Closure	1.23
LOSP	0.17
Turbine Trip	8.17

Table B.2 Functions and Systems

Notation	Function	System
C	Reactor Subcriticality	RPS
Q	Feedwater Injection	COND/FW+PCS
U	High Pressure Injection	HPCI.RCIC
V	Low Pressure Injection	LPCI.LPCS
X	Manual ADS Depressurization	Operator
W	Containment Heat Removal	(RHR+RHRSW).PCS
C'	Poison Injection	SLCS
U_H	High Pressure Injection	HPCI
U_R	High Pressure Injection	RCIC
D	ADS Inhibition	ADS+Operator
W_{12}	Containment Heat Removal	RHR

Table B.3 List of "Components"

X(I)	Name	Event Description
1	RPS(M)	Mechanical failure of reactor protection system
2	SLCSH	Hardware failure of standby liquid control system
3	LOSP	Transient induced loss of offsite power
4	EDC	Loss of all DC (loss of all AC for more than four hours or other failures in DC power supply system)
5	WSW	Loss of service water
6	FWPCS	Hardware failure of the feedwater and PCS system
7	ARC	Operator failure to provide alternate room cooling to frontline system rooms
8	RCICH	Hardware failure of reactor core isolation cooling system
9	HPCIH	Hardware failure of high pressure coolant injection system
10	ADSH	Hardware failure of automatic depressurization system
11	LPCIH	Hardware failure of low pressure coolant injection system
12	LPCSH	Hardware failure of low pressure core spray system
13	RECOV	Failure to recover the support systems
14	RHRH	Hardware failure of residual heat removal system
15	FWPCSL	Hardware failure of feedwater and PCS system for long-term containment heat removal
16	DG	Failure of diesel generator system
17	X	Operator failure to actuate the ADS
18	D	Operator failure to inhibit ADS actuation in ATWS events
19	FWPCSL(RECOV)	Failure to recover feedwater and PCS hardware in 20 hours given that it failed in early phase (Q)
20	$\hat{A}$	Median ground acceleration capacity of reactor enclosure and control structure
21	β_R	Logarithmic standard deviation associated with the underlying randomness of the capacity for the reactor enclosure and control structure
22	S	Containment failure

Table B.4 Reliability Cost Functions

	Component	a_i	b_i
1	RPS(M)	10.	0.
2	SLCSH	1.	0.
3	LOSP	1.	0.
4	EDC	1.	0.
5	WSW	1.	0.
6	FWPCS	10.	0.
7	ARC	1.	0.
8	RCICH	1.	0.
9	HPSIH	1.	0.
10	ADSH	1.	0.
11	LPCIH	1.	0.
12	LPCSH	1.	0.
13	RECOV	10.	0.
14	RHRH	10.	0.
15	FWPCSL	10.	0.
16	DG	10.	0.
17	X	1.	0.
18	D	1.	0.
19	FWPCSL(RECOV)	10.	0.
20	A	50.	0.
21	β_R	50.	0.
22	S	10^5	0.

Table B.5 Input Range of Component Unavailabilities

X(I)	Name	Model Plant Nominal Mean Unavailability	Lower Limit	Upper Limit
1	RPS(M)	1.0(-5)	1.0(-7)	1.0
2	SLCSH	3.5(-3)	1.0(-4)	1.0
3	LOSP	5.2(-4)	5.2(-4)(Fixed)	5.2(-4)
4	EDC	2.5(-7)	1.0(-7)	1.0
5	WSW	5.0(-7)	1.0(-7)	1.0
6	FWPCS	2.0(-2)	5.0(-3)	1.0
7	ARC	1.5(-1)	1.5(-1)(Fixed)	1.5(-1)
8	RCICH	7.0(-2)	1.0(-2)	1.0
9	HPCIH	1.16(-1)	1.0(-2)	1.0
10	ADSH	1.76(-4)	1.0(-5)	1.0
11	LPCIH	1.8(-3)	1.0(-4)	1.0
12	LPCSH	2.6(-3)	1.0(-4)	1.0
13	RECOV	1.7(-1)	5.0(-2)	1.0
14	RHRH	4.5(-5)	1.0(-5)	1.0
15	FWPCSL	6.0(-2)	1.0(-3)	1.0
16	DG	9.7(-4)	1.0(-4)	1.0
17	X	6.0(-3)	1.0(-10)*	1.0
18	D	2.0(-3)	2.0(-3)(Fixed)	2.0(-3)
19	FWPCSL(RECOV)	3.6(-1)	5.0(-2)	1.0
20	$\hat{A}$	1.05	1.0(-1)	3.1 (-1)
21	β_R	3.1(-1)	3.1(-1)(Fixed)	3.1(-1)
22	S	1.0(-1)	1.0(-4)	1.0

*The design of the plant provides for an automatic initiation of depressurization for LOCA initiators. Transient initiators, however, require manual initiation. A low value of X means that the need for manual initiation has been removed and that automatic initiation is provided for transient initiators.

Table B.6 Site Matrices (Ref. 4)

	Lower-estimate		Best-estimate		Upper-estimate	
	A	L	A	L	A	L
R_1	0.	1.58(+1)	0.	2.16(+3)	1.43(+0)	9.42(+3)
R_{2a}	2.12(+2)	2.13(+3)	2.12(+2)	2.13(+4)	2.12(+2)	2.13(+4)
R_{2b}	7.95(+1)	1.77(+4)	7.95(+1)	1.77(+4)	7.95(+1)	1.77(+4)
R_{2c}	9.43(+1)	1.84(+4)	9.43(+1)	1.84(+4)	9.43(+1)	1.84(+4)
R_{2d}	6.04(-1)	6.62(+3)	6.04(-1)	6.62(+3)	6.04(-1)	6.62(+3)
R_3	0.	4.67(+3)	7.54(+1)	1.40(+4)	7.54(+1)	1.40(+4)
R_4	0.	4.67(+3)	6.89(+1)	1.40(+4)	6.89(+1)	1.40(+4)
R_5	0.	1.29(+4)	1.38(+2)	1.29(+4)	1.38(+2)	1.29(+4)
R_6	2.00(+3)	3.00(+3)	2.00(+3)	3.00(+3)	2.00(+3)	3.00(+3)

Table B.7 Containment Matrix*

	R_1	R_{2a}	R_{2b}	R_{2c}	R_{2d}	R_3	R_4	R_5	R_6
I.	.775	α_1	0	0	$\beta_1\mu'$	0	0	0	0
II.	.445	0	α_2	0	$\beta_2\mu'$	0	0	0	0
III.	.775	α_1	0	0	$\beta_1\mu'$	0	0	0	0
IV.	0	0	0	α_2	$\beta_2\mu'$	γ	γ'	γ''	0
V.	0	0	0	0	0	0	0	0	1

*The element c_{jr} of the containment matrix denotes the conditional probability that given plant damage site j, the rth radioactivity release will result.

Table B.8 Noninferior Solutions at Core Damage Frequency 1.0(-3) for the Extended Model

	A1	A2	A3	A4	A5
C_d	1.00(-3)	1.00(-3)	1.00(-3)	1.00(-3)	1.00(-3)
A	1.67(-2)	2.00(-2)	2.50(-2)	3.00(-2)	5.65(-2)
L	4.23(+0)	4.74(+0)	5.50(+0)	6.25(+0)	1.02(+1)
G	5.10(+4)	4.87(+4)	4.67(+4)	4.56(+4)	4.40(+4)
X(1)	7.87(-4)	9.79(-4)	1.27(-3)	1.55(-3)	3.04(-3)
X(2)	2.21(-3)	1.97(-3)	1.71(-3)	1.50(-3)	1.05(-3)
X(3)	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)
X(4)	5.74(-5)	5.68(-5)	5.62(-5)	5.56(-5)	5.33(-5)
X(5)	1.26(-4)	1.26(-4)	1.25(-4)	1.24(-4)	1.19(-4)
X(6)	8.23(-3)	8.33(-3)	8.40(-3)	8.41(-3)	8.32(-3)
X(7)	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)
X(8)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	1.49(-2)	1.45(-2)	1.43(-2)	1.42(-2)	1.36(-2)
X(11)	6.18(-2)	6.14(-2)	6.01(-2)	6.04(-2)	5.82(-2)
X(12)	5.81(-2)	5.76(-2)	5.70(-2)	5.69(-2)	5.56(-2)
X(13)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	3.26(-3)	3.29(-3)	3.30(-3)	3.30(-3)	3.20(-3)
X(15)	5.45(-3)	5.52(-3)	5.56(-3)	5.57(-3)	5.51(-3)
X(16)	3.47(-3)	3.43(-3)	3.39(-3)	3.36(-3)	3.22(-3)
X(17)	1.49(-2)	1.45(-2)	1.43(-2)	1.42(-2)	1.36(-2)
X(18)	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)
X(19)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)
X(20)	1.30(+0)	1.28(+0)	1.23(+0)	1.17(+0)	9.30(-1)
X(21)	3.10(-1)	3.10(-1)	3.10(-1)	3.10(-1)	3.10(-1)
X(22)	1.00(-0)	1.00(-0)	1.00(-0)	1.00(-0)	1.00(-0)

Table B.9 Noninferior Solutions at Core Damage Frequency 1.0(-4) for the Extended Model

	C1	C2	C3	C4	C5
C_d	1.00(-4)	1.00(-4)	1.00(-4)	1.00(-4)	1.00(-4)
A	1.25(-4)	2.00(-4)	4.17(-4)	1.00(-3)	6.69(-3)
L	1.74(-1)	1.86(-1)	2.19(-1)	3.11(-1)	1.18(+0)
G	1.43(+6)	1.03(+6)	7.05(+5)	5.02(+5)	3.53(+5)
X(1)	2.21(-5)	3.03(-5)	4.63(-5)	7.31(-5)	3.66(-4)
X(2)	1.53(-3)	1.21(-3)	9.81(-4)	7.62(-4)	3.16(-4)
X(3)	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)
X(4)	6.64(-6)	6.39(-6)	6.17(-6)	6.02(-6)	5.57(-6)
X(5)	1.13(-5)	1.22(-5)	1.29(-5)	1.31(-5)	1.25(-5)
X(6)	5.00(-3)	5.00(-3)	5.00(-3)	5.00(-3)	5.00(-3)
X(7)	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)
X(8)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	1.70(-3)	1.61(-3)	1.58(-3)	1.54(-3)	1.46(-3)
X(11)	1.46(-2)	1.43(-2)	1.39(-2)	1.39(-2)	1.31(-2)
X(12)	1.37(-2)	1.34(-2)	1.31(-2)	1.28(-2)	1.23(-2)
X(13)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	3.43(-4)	4.12(-4)	4.86(-4)	5.34(-4)	5.40(-4)
X(15)	1.05(-3)	1.18(-3)	1.30(-3)	1.38(-3)	1.40(-3)
X(16)	4.01(-4)	3.86(-4)	3.72(-4)	3.63(-4)	3.36(-4)
X(17)	1.71(-3)	1.66(-3)	1.58(-3)	1.60(-3)	1.40(-3)
X(18)	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)
X(19)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)
X(20)	1.50(+0)	1.50(+0)	1.50(+0)	1.50(+0)	1.34(+0)
X(21)	3.10(-1)	3.10(-1)	3.10(-1)	3.10(-1)	3.10(-1)
X(22)	1.31(-1)	2.01(-1)	3.49(-1)	6.22(-1)	1.00(-0)

Table B.10 Noninferior Solutions at Core Damage Frequency 5.0(-5) for the Extended Model

	D1	D2	D3	D4	D5
C_d	5.00(-5)	5.00(-5)	5.00(-5)	5.00(-5)	5.00(-5)
A	5.83(-5)	8.33(-5)	1.00(-4)	1.00(-3)	3.43(-3)
L	8.34(-2)	8.67(-2)	8.92(-2)	2.29(-1)	6.00(-1)
G	2.23(+6)	2.08(+6)	1.80(+6)	7.85(+5)	6.88(+5)
X(1)	1.01(-5)	1.57(-5)	1.84(-5)	6.95(-5)	1.87(-4)
X(2)	1.15(-3)	8.72(-4)	7.92(-4)	3.83(-4)	2.21(-4)
X(3)	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)
X(4)	3.37(-6)	3.19(-6)	3.14(-6)	2.95(-6)	2.80(-6)
X(5)	5.45(-6)	6.17(-6)	6.32(-6)	6.56(-6)	6.25(-6)
X(6)	5.00(-3)	5.00(-3)	5.00(-3)	5.00(-3)	5.00(-3)
X(7)	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)
X(8)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	8.65(-4)	8.22(-4)	8.09(-4)	7.60(-4)	7.20(-4)
X(11)	9.10(-3)	8.85(-3)	8.85(-3)	8.26(-3)	7.91(-3)
X(12)	8.79(-3)	8.52(-3)	8.50(-3)	8.41(-3)	8.17(-3)
X(13)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	1.62(-4)	2.16(-4)	2.34(-4)	2.98(-4)	2.88(-4)
X(15)	1.00(-3)	1.00(-3)	1.00(-3)	1.00(-3)	1.00(-3)
X(16)	2.03(-4)	1.93(-4)	1.90(-4)	1.78(-4)	1.69(-4)
X(17)	8.65(-4)	8.22(-4)	8.09(-4)	7.60(-4)	7.20(-4)
X(18)	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)
X(19)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)
X(20)	1.50(+0)	1.50(+0)	1.50(+0)	1.50(+0)	1.45(+0)
X(21)	3.10(-1)	3.10(-1)	3.10(-1)	3.10(-1)	3.10(-1)
X(22)	5.79(-2)	1.05(-1)	1.30(-1)	7.16(-1)	1.00(-0)

Table B.11 List of "Components"

X(I)	Name	Event Description
1	RPS(M)	Mechanical failure of reactor protection system
2	SLCSH	Hardware failure of standby liquid control system
3	LOSP	Transient induced loss of offsite power
4	EDC	Loss of all DC (loss of all AC for more than four hours or other failures in DC power supply system)
5	WSW	Loss of service water
6	FWPCS	Hardware failure of the feedwater and PCS system
7	ARC	Operator failure to provide alternate room cooling to frontline system rooms
8	RCICH	Hardware failure of reactor core isolation cooling system
9	HPCIH	Hardware failure of high pressure coolant injection system
10	ADSH	Hardware failure of automatic depressurization system
11	LPCIH	Hardware failure of low pressure coolant injection system
12	LPCSH	Hardware failure of low pressure core spray system
13	RECOV	Failure to recover the support systems
14	RHRH	Hardware failure of residual heat removal system
15	FWPCSL	Hardware failure of feedwater and PCS system for long-term containment heat removal
16	DG	Failure of diesel generator system
17	X	Operator failure to actuate the ADS
18	D	Operator failure to inhibit ADS actuation in ATWS events
19	FWPCSL(RECOV)	Failure to recover feedwater and PCS hardware in 20 hours given that it failed in early phase (Q)
20	$\hat{A}$	Median ground acceleration capacity of reactor enclosure and control structure
21	β_R	Logarithmic standard deviation associated with the underlying randomness of the capacity for the reactor enclosure and control structure
22	γ	Drywell overpressure failure
23	γ'	Wetwell overpressure failure
24	γ''	Suppression pool failure
25	μ'	Hydrogen detonation
26	α_1	In-vessel steam explosion in Classes I or III
27	α_2	In-vessel steam explosion in Classes II or IV
28	β_1	Ex-vessel steam explosion in Classes I or III
29	β_2	Ex-vessel steam explosion in Classes II or IV

Table B.12 Nominal Reliability Cost Functions

	Component	Cost Model	a_i	b_i
1	RPS(M)	$a_i(1/x_i - 1) + b_i$	10.	0.
2	SLCSH	"	1.	0.
3	LOSP	"	1.	0.
4	EDC	"	1.	0.
5	WSW	"	1.	0.
6	FWPCS	"	10.	0.
7	ARC	"	1.	0.
8	RCICH	"	1.	0.
9	HPSIH	"	1.	0.
10	ADSH	"	1.	0.
11	LPCIH	"	1.	0.
12	LPCSH	"	1.	0.
13	RECOV	"	10.	0.
14	RHRH	"	10.	0.
15	RWPCSL	"	10.	0.
16	DG	"	10.	0.
17	X	"	1.	0.
18	D	"	1.	0.
19	FWPCSL(RECOV)	"	10.	0.
20	$\hat{A}$	$a_i/(1.6 - x_i) + b_i$	50.	0.
21	β_R	$a_i/x_i + b_i$	50.	0.
22	γ	$a_i(1/x_i - 1) + b_i$	200.	200.
23	γ'	"	200.	200.
24	γ''	"	200.	200.
25	μ'	"	200.	200.
26	α_1	"	100.	100.
27	α_2	"	200.	200.
28	β_1	"	100.	100.
29	β_2	"	200.	200.

Table B.13 Reliability Cost Functions for a Sensitivity Calculation*

Component	Cost Model	a_i	b_i
22	$a_i(1/\sqrt{x_i}-1) + b_i$	200.	200.
23	"	200.	200.
24	"	200.	200.
25	"	200.	200.
26	"	100.	100.
27	"	200.	200.
28	"	100.	100.
29	"	200.	200.

*Same with those in Table B.12 otherwise.

Table B.14 Reliability Cost Functions for a Sensitivity Calculation**

Component	Cost Model	a_i	b_i
22	$a_i(1/x_i-1) + b_i$	100.	100.
23	"	100.	100.
24	"	100.	100.
25	"	100.	100.
26	"	50.	50.
27	"	100.	100.
28	"	50.	50.
29	"	100.	100.

**Same with those in Table 12 otherwise.

Table B.15 Reliability Cost for Diesel Generator System as a Function of Unavailability Used in a Sensitivity Calculation*

X(16)	$g_i[X(16)]$
1.00(-4)	2.00(+4)
2.00(-4)	1.00(+4)
3.00(-4)	6.70(+3)
4.00(-4)	5.00(+3)
7.00(-4)	3.00(+3)
8.00(-4)	2.70(+3)
1.00(-3)	2.30(+3)
1.50(-3)	1.80(+3)
3.00(-3)	1.45(+3)
7.00(-3)	1.07(+3)
8.00(-3)	1.00(+3)
1.00(-2)	9.00(+2)
1.30(-2)	7.40(+2)
2.00(-2)	5.00(+2)
5.00(-2)	2.00(+2)
1.00(-1)	1.00(+2)
2.00(-1)	5.00(+1)
5.00(-1)	2.00(+1)
1.00(-0)	1.00(+1)

*Same with those in Table B.12 otherwise.

Table B.16 Input Range of Component Unavailabilities*

X(I)	Name	Model Plant Nominal Mean Unavailability	Lower Limit	Upper Limit
1	RPS(M)	1.0(-5)	1.0(-7)	1.0
2	SLCSH	3.5(-3)	1.0(-4)	1.0
3	LOSP	5.2(-4)	5.2(-4)(Fixed)	5.2(-4)
4	EDC	2.5(-7)	1.0(-7)	1.0
5	WSW	5.0(-7)	1.0(-7)	1.0
6	FWPCS	2.0(-2)	5.0(-3)	1.0
7	ARC	1.5(-1)	1.5(-1)(Fixed)	1.5(-1)
8	RCICH	7.0(-2)	1.0(-2)	1.0
9	HPCIH	1.16(-1)	1.0(-2)	1.0
10	ADSH	1.76(-4)	1.0(-5)	1.0
11	LPCIH	1.8(-3)	1.0(-4)	1.0
12	LPCSH	2.6(-3)	1.0(-4)	1.0
13	RECOV	1.7(-1)	5.0(-2)	1.0
14	RHRH	4.5(-5)	1.0(-5)	1.0
15	FWPCSL	6.0(-2)	1.0(-3)	1.0
16	DG	9.7(-4)	1.0(-4)	1.0
17	X	6.0(-3)	1.0(-10)*	1.0
18	D	2.0(-3)	2.0(-3)(Fixed)	2.0(-3)
19	FWPCSL(RECOV)	3.6(-1)	5.0(-2)	1.0
20	$\hat{A}$	1.05	1.0(-1)	3.1(-1)
21	β_R	3.1(-1)	3.1(-1)(Fixed)	3.1(-1)
22	γ	4.45(-1)	1.0(-4)	1.0
23	γ'	2.23(-1)	1.0(-4)	1.0
24	γ''	2.23(-1)	1.0(-4)	1.0
25	μ'	1.00(-1)	1.0(-4)	1.0
26	α_1	1.00(-3)	1.0(-4)	1.0
27	α_2	1.00(-2)	1.0(-4)	1.0
28	β_1	1.00(-3)	1.0(-4)	1.0
29	β_2	1.00(-1)	1.04(-4)	1.0

*The design of the plant provides for an automatic initiation of depressurization for LOCA initiators. Transient initiators, however, require manual initiation. A low value of X means that the need for manual initiation has been removed and that automatic initiation is provided for transient initiators.

Table B.17 Ranges* of Unavailabilities from Sensitivity Calculations with the Extended Model

X(i)	Name	X_L	X_u
1	RPS(M)	1.09(-4)	3.55(-4)
2	SLCSH	3.33(-4)	6.45(-4)
4	EDC	5.63(-6)	6.26(-6)
5	WSW	1.24(-5)	1.34(-5)
6	FWPCS	5.00(-3)	5.00(-3)
8	RCICH	1.00(-2)	1.00(-2)
9	HPCIH	1.00(-2)	1.00(-2)
10	ADSH	1.44(-3)	1.62(-3)
11	LPCIH	3.40(-3)	1.39(-2)
12	LPCSH	4.17(-3)	1.34(-2)
13	RECOV	5.00(-2)	5.00(-2)
14	RHRH	4.39(-4)	5.80(-4)
15	FWPCSL	1.23(-3)	1.46(-3)
16	DG	1.82(-4)	3.73(-4)
17	X	1.41(-3)	1.90(-3)
19	FWPCSL(RECOV)	5.00(-2)	5.00(-2)
20	$\hat{A}$	1.50(+0)	1.50(+0)
22	γ	2.87(-3)	1.00(-0)
23	γ'	3.01(-3)	1.00(-0)
24	γ''	3.19(-3)	1.00(-0)
25	μ'	3.23(-2)	1.13(-1)
26	α_1	1.61(-4)	1.69(-3)
27	α_2	1.31(-3)	8.36(-3)
28	β_1	3.14(-2)	9.69(-2)
29	β_2	1.20(-1)	3.09(-1)

*Among lower limit noninferior solutions of acute and latent fatalities at C_d = 1.00(-4).

Table B.18 Ranges* of Unavailabilities from Sensitivity Calculations with the Extended Model

X(i)	Name	X_L	X_u
1	RPS(M)	3.66(-4)	3.83(-4)
2	SLCSH	3.15(-4)	3.23(-4)
4	EDC	5.57(-6)	5.83(-6)
5	WSW	1.25(-5)	1.30(-5)
6	FWPCS	5.00(-3)	5.00(-3)
8	RCICH	1.00(-2)	1.00(-2)
9	HPCIH	1.00(-2)	1.00(-2)
10	ADSH	1.43(-3)	1.50(-3)
11	LPCIH	1.27(-2)	1.34(-2)
12	LPCSH	1.21(-2)	1.34(-2)
13	RECOV	5.00(-2)	5.00(-2)
14	RHRH	5.40(-4)	5.63(-4)
15	FWPCSL	1.40(-3)	1.44(-3)
16	DG	1.69(-4)	3.36(-4)
17	X	1.43(-3)	1.50(-3)
19	FWPCSL(RECOV)	5.00(-2)	5.00(-2)
20	$\hat{A}$	1.34(+0)	1.35(+0)
22	γ	1.00(-0)	1.00(-0)
23	γ'	1.00(-0)	1.00(-0)
24	γ''	1.00(-0)	1.00(-0)
25	μ'	1.00(-0)	1.00(-0)
26	α_1	1.00(-0)	1.00(-0)
27	α_2	1.00(-0)	1.00(-0)
28	β_1	9.74(-1)	1.00(-0)
29	β_2	1.00(-0)	1.00(-0)

*Among upper limit noninferior solutions of acute and latent fatalities at C_d = 1.00(-4).

Table B.19 List of "Components"

X(I)	Name	Event Description
1	RPS(M)	Mechanical failure of reactor protection system
2	SLCSH	Hardware failure of standby liquid control system
3	LOSP	Transient induced loss of offsite power
4	EDC	Loss of all DC (loss of all AC for more than four hours or other failures in DC power supply system)
5	WSW	Loss of service water
6	FWPCS	Hardware failure of the feedwater and PCS system
7	ARC	Operator failure to provide alternate room cooling to frontline system rooms
8	RCICH	Hardware failure of reactor core isolation cooling system
9	HPCIH	Hardware failure of high pressure coolant injection system
10	ADSH	Hardware failure of automatic depressurization system
11	LPCIH	Hardware failure of low pressure coolant injection system
12	LPCSH	Hardware failure of low pressure core spray system
13	RECOV	Failure to recover the support systems
14	RHRH	Hardware failure of residual heat removal system
15	FWPCSL	Hardware failure of feedwater and PCS system for long-term containment heat removal
16	DG	Failure of diesel generator system
17	X	Operator failure to actuate the ADS
18	D	Operator failure to inhibit ADS actuation in ATWS events
19	FWPCSL(RECOV)	Failure to recover feedwater and PCS hardware in 20 hours given that it failed in early phase (Q)
20	C_E	Electrical failure of reactor protection system.
21	K^E	Failure of alternate rod insertion.
22	C"	Operator failure to timely scram.
23	P	Failure of safety-relief valves to reclose.
24	M	Failure of adequate pressure control.

Table B.20 Comparison of Noninferior Solutions Between the Base Model and Two Model Sensitivity Studies

	A6	A6'	A6"
C_d	1.00(-3)	1.00(-3)	1.00(-3)
A	4.93(-3)	4.98(-3)	5.47(-3)
L	2.32(0)	2.33(0)	2.40(0)
G	4.37(+4)	4.38(+4)	4.47(+4)
X(1)	3.04(-3)	3.01(-3)	2.87(-3)
X(2)	1.05(-3)	1.05(-3)	1.05(-3)
X(3)	5.20(-4)	5.20(-4)	5.20(-4)
X(4)	5.33(-5)	5.33(-5)	5.30(-5)
X(5)	1.19(-4)	1.19(-4)	1.19(-4)
X(6)	8.32(-3)	8.35(-3)	8.28(-3)
X(7)	1.50(-1)	1.50(-1)	1.50(-1)
X(8)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	1.36(-2)	1.36(-2)	1.34(-2)
X(11)	5.79(-2)	5.78(-2)	6.25(-2)
X(12)	5.62(-2)	5.61(-2)	6.04(-2)
X(13)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	3.20(-3)	3.16(-3)	3.19(-3)
X(15)	5.51(-3)	5.53(-3)	5.48(-3)
X(16)	3.22(-3)	3.22(-3)	3.20(-3)
X(17)	1.36(-2)	1.36(-2)	1.39(-2)
X(18)	2.00(-3)	2.00(-3)	2.00(-3)
X(19)	5.00(-2)	5.00(-2)	5.00(-2)
X(20)	--	--	1.10(-2)
X(21)	--	--	6.52(-2)
X(22)	--	--	5.57(-3)
X(23)	--	--	5.75(-1)
X(24)	--	--	5.54(-3)

Table B.21 Comparison of Noninferior Solutions Between the Base Model and Two Model Sensitivity Studies

	B5	B5'	B5"
C_d	5.00(-4)	5.00(-4)	5.00(-4)
A	2.66(-3)	2.68(-3)	2.85(-3)
L	1.19(0)	1.20(0)	1.22(0)
G	7.95(+4)	7.97(+4)	8.08(+4)
X(1)	1.65(-3)	1.63(-3)	1.58(-3)
X(2)	7.27(-4)	7.30(-4)	7.26(-4)
X(3)	5.20(-4)	5.20(-4)	5.20(-4)
X(4)	2.73(-5)	2.72(-5)	2.71(-5)
X(5)	6.10(-5)	6.09(-5)	6.07(-5)
X(6)	5.31(-3)	5.35(-3)	5.29(-3)
X(7)	1.50(-1)	1.50(-1)	1.50(-1)
X(8)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	6.79(-3)	7.00(-3)	6.80(-3)
X(11)	3.75(-2)	3.74(-2)	3.99(-2)
X(12)	3.56(-2)	3.58(-2)	3.81(-2)
X(13)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	2.05(-3)	2.02(-3)	2.05(-3)
X(15)	3.52(-3)	3.54(-3)	3.50(-3)
X(16)	1.65(-3)	1.64(-3)	1.64(-3)
X(17)	7.44(-3)	7.00(-3)	7.07(-3)
X(18)	2.00(-3)	2.00(-3)	2.00(-3)
X(19)	5.00(-2)	5.00(-2)	5.00(-2)
X(20)	--	--	8.17(-3)
X(21)	--	--	4.70(-2)
X(22)	--	--	3.76(-3)
X(23)	--	--	3.86(-1)
X(24)	--	--	3.86(-3)

Table B.22 Comparison of Noninferior Solutions Between the Base Model and Two Model Sensitivity Studies

	C8	C8'	C8"
C_d	1.00(-4)	1.00(-4)	1.00(-4)
A	5.87(-4)	5.93(-4)	6.04(-4)
L	2.47(-1)	2.48(-1)	2.49(-1)
G	3.52(+5)	3.53(+5)	3.55(+5)
X(1)	3.66(-4)	3.62(-4)	3.58(-4)
X(2)	3.15(-4)	3.16(-4)	3.12(-4)
X(3)	5.20(-4)	5.20(-4)	5.20(-4)
X(4)	5.57(-6)	5.56(-6)	5.56(-6)
X(5)	1.25(-5)	1.24(-5)	1.24(-5)
X(6)	5.00(-3)	5.00(-3)	5.00(-3)
X(7)	1.50(-1)	1.50(-1)	1.50(-1)
X(8)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	1.43(-3)	1.43(-3)	1.43(-3)
X(11)	1.31(-2)	1.30(-2)	1.28(-2)
X(12)	1.23(-2)	1.24(-2)	1.26(-2)
X(13)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	5.40(-4)	5.28(-4)	5.39(-4)
X(15)	1.40(-3)	1.41(-3)	1.40(-3)
X(16)	3.36(-4)	3.36(-4)	3.36(-4)
X(17)	1.43(-3)	1.43(-3)	1.43(-3)
X(18)	2.00(-3)	2.00(-3)	2.00(-3)
X(19)	5.00(-2)	5.00(-2)	5.00(-2)
X(20)	--	--	4.01(-3)
X(21)	--	--	2.01(-2)
X(22)	--	--	1.64(-3)
X(23)	--	--	5.01(-1)
X(24)	--	--	1.64(-3)

Table B.23 Comparison of Noninferior Solutions Between the Base Model and Two Model Sensitivity Studies

	D8	D8'	D8"
C_d	5.00(-5)	5.00(-5)	5.00(-5)
A	3.01(-4)	3.04(-4)	3.07(-4)
L	1.24(-1)	1.25(-1)	1.25(-1)
G	6.87(+5)	6.89(+5)	6.91(+5)
X(1)	1.88(-4)	1.85(-4)	1.85(-4)
X(2)	2.21(-4)	2.22(-4)	2.19(-4)
X(3)	5.20(-4)	5.20(-4)	5.20(-4)
X(4)	2.80(-6)	2.79(-6)	2.79(-6)
X(5)	6.26(-6)	6.25(-6)	6.25(-6)
X(6)	5.00(-3)	5.00(-3)	5.00(-3)
X(7)	1.50(-1)	1.50(-1)	1.50(-1)
X(8)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	7.20(-4)	7.19(-4)	7.16(-4)
X(11)	7.99(-3)	7.96(-3)	8.18(-3)
X(12)	8.09(-3)	8.10(-3)	8.41(-3)
X(13)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	2.89(-4)	2.82(-4)	2.88(-4)
X(15)	1.00(-3)	1.00(-3)	1.00(-3)
X(16)	1.69(-4)	1.69(-4)	1.69(-4)
X(17)	7.20(-4)	7.18(-4)	7.25(-4)
X(18)	2.00(-3)	2.00(-3)	2.00(-3)
X(19)	5.00(-2)	5.00(-2)	5.00(-2)
X(20)	--	--	2.87(-3)
X(21)	--	--	1.39(-2)
X(22)	--	--	1.14(-3)
X(23)	--	--	1.66(-1)
X(24)	--	--	1.17(-3)

Table B.24 Aspiration Levels After Preliminary Screening for Base Model and Sensitivity Models

	Base Model		Case 1		Case 2	
	X_L	X_U	X_L	X_U	X_L	X_U
X(1)	1.88(-4)	3.04(-3)	1.85(-4)	3.01(-3)	1.85(-4)	2.87(-3)
X(2)	2.21(-4)	1.05(-3)	2.22(-4)	1.05(-3)	2.19(-4)	1.05(-3)
X(4)	2.80(-6)	5.33(-5)	2.79(-6)	5.33(-5)	2.79(-6)	5.30(-5)
X(5)	6.26(-6)	1.19(-4)	6.25(-6)	1.19(-4)	6.25(-6)	1.19(-4)
X(6)	5.00(-3)	8.32(-3)	5.00(-3)	8.35(-3)	5.00(-3)	8.28(-3)
X(8)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	7.20(-4)	1.36(-2)	7.19(-4)	1.36(-2)	7.16(-4)	1.34(-2)
X(11)	7.99(-3)	5.79(-2)	7.96(-3)	5.78(-2)	8.18(-3)	6.25(-2)
X(12)	8.09(-3)	5.62(-2)	8.10(-3)	5.61(-2)	8.41(-3)	6.04(-2)
X(13)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	2.89(-4)	3.20(-3)	2.82(-4)	3.16(-3)	2.88(-4)	3.19(-3)
X(15)	1.00(-3)	5.51(-3)	1.00(-3)	5.53(-3)	1.00(-3)	5.48(-3)
X(16)	1.69(-4)	3.22(-3)	1.69(-4)	3.22(-3)	1.69(-4)	3.20(-3)
X(17)	7.20(-4)	1.36(-2)	7.18(-4)	1.36(-2)	7.25(-4)	1.39(-2)
X(19)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)

APPENDIX C

PREFERENCE ASSESSMENT

C.1 Introduction

The methodology we developed in Section 2 and Appendix A for the reliability allocation program does not attempt to find the best (optimal) solution in a single stroke, rather it is formulated to generate or identify all (in reality, as many as the analyst or the decision maker desires) noninferior outcomes and corresponding decision variables.

The identification of the noninferior solutions was accomplished through the mean-to-mean mapping between the outcome variables and the decision variables. This was possible because, in general, the PRA models retain the closure property, i.e., the top level criteria are also mean values when the allocated component reliabilities are mean values (see Section A.5).

Once the set of noninferior solutions is assessed, a choice among the elements of this set is necessary. In Section 3.1 we were able to discard some of the noninferior solution set and we were left with a smaller noninferior solution set without a formal preference assessment by the decision maker. There is no guarantee, however, that such an approach of informal preference assessment will be possible in the general case and hence a formal preference assessment for the ultimate resolution of such a decision problem would be desirable.

The preference assessment in the outcome space is a rather involved task, both because of the multitude of the attributes and because the decision maker is not a single individual. The society expresses its preferences through the various bodies (e.g., NRC, industry, intervenors). The primary motivation of our current approach was to give a full exposition of the problem to the decision maker and to those who have to accept the decision. The basic premise here is, following the value theory of information, that the more is understood about the decision problem, the easier preferences on the outcomes can be articulated and understood. Therefore, the presentation of all noninferior solutions would facilitate the process of assessing and communicating the corresponding preferences.

We have examined to a limited extent the problem of preference assessment in the context of decision analysis.[21] The following is a brief survey.

Most approaches in decision analysis start with a set of axioms regarding the decision maker's preference structure, which will lead to the existence of a preference function (called value function in the case of decision under certainty, or utility function in the case of decision under uncertainty). The axioms are some mild conditions on a decision maker's decision making process so that his preference structure can be represented by a preference function. In essence, these axioms are equivalent to assuming that the decision maker is rational and consistent in a decision-making process.

In a multiattribute decision problem, the decision analysis usually[13] invokes further assumptions of preferential independence, utility independence,

and additive independence in order to specify the preference function to a family of parametric functions, e.g., additive or multiplicative form of unidimensional preference functions, and then concentrates on the assessment of the unidimensional preference functions. The assessment of the unidimensional preference function will be a much easier task than the assessment of the multidimensional (multiattribute) preference function (this is in a sense, a decomposition approach). This is so, because the assumption of preferential independence or utility independence means that, crudely, the decision maker's preference between two outcomes given that the other outcomes are held fixed does not depend on the levels at which the other outcomes are held fixed.

Once the preference function has been obtained in a combination of unidimensional preference functions, the decision problem becomes a standard single objective optimization problem.

The next section briefly describes an alternative approach to the usual approaches above, which was suggested by one of the steering group members.

C.2 Decomposition Approach

The starting point of Boyd[22] is the same as with the usual decision analysis. The departure of Boyd from other methods of decision analysis is, however, in the way the preference function is assessed. Rather than assessing the unidimensional preference functions by invoking seemingly strong assumptions of preferential and utility independence, he assesses "local" (in outcome space) trade-off ratios iteratively under milder conditions on the decision maker's preference ordering. These mild conditions are: (1) Differentiability of preference function, (2) Convexity of preference relation, and (3) No satiation outcome.

Operationally, Boyd's procedure for assessment of risk preferences (utility functions) is decomposed into:

Step 1

a. an evaluation of deterministic trade-offs, and
b. an assessment of risk preference on an appropriately chosen, real-valued numeraire.

For most of the real problems, the direct evaluation of deterministic trade-offs is a difficult task. For these cases, Step 1a can be further decomposed through an iterative pricing scheme where at each iteration:

Step 2

a. assess deterministic trade-offs in the form of generalized prices, and
b. solve a relatively simple profit maximization problem.

The iterative pricing scheme is based on the idea that rather than maximizing directly the value function $v[\underline{Z}(\underline{X})]$ which is not itself known explicitly, it is to maximize the "profit" received as a result of the decision. In other words, one of the outcome variables, say Z_p, is taken as a price variable; all the other outcome variables are "priced" in terms of this variable;

and the resulting profit is maximized. The resulting profit could be written as

$$v[\underline{Z}(\underline{X})] = \sum_{k=1}^{p} \lambda_k Z_k(\underline{X})$$

where λ_k is the trade-off ratio, i.e., units of p^{th} variable that the decision maker would give up to receive one additional unit of the k^{th} variable.

The decision maker should articulate the λ_k's. Since it would be too fortunate for the decision maker to guess the "right" prices, the assessment of the λ_k's would involve some kind of iteration. Boyd provides the following theorem and an algorithm based on it for this purpose (reproduced here in our notation):

Theorem I

If the decision maker's preference ordering satisfies the conditions (1), (2), and (3) on the previous page, and if $\underline{X}^*$ maximizes

$H = \sum_{k=1}^{p} \lambda_k[Z(\underline{X}^*)]Z_k(\underline{X})$ over all $\underline{X} \in F_d$, then $\underline{X}^*$ also maximizes

$v[\underline{Z}(\underline{X})]$ over all $\underline{x} \in F_d$,

where

$$\lambda_k[\underline{Z}(\underline{X})] = \left.\frac{\partial v(\underline{Z})/\partial Z_k}{\partial v(\underline{Z})/\partial Z_p}\right|_{\underline{Z} = \underline{Z}(\underline{X})} = \left. -\frac{dZ_p}{dZ_k}\right|_{v, Z_j (j \neq k, p) = \text{constant}}.$$

Successive Approximation Algorithm

1. Choose an arbitrary initial decision vector $\underline{X}^\circ$ and get the decision maker to evaluate the corresponding $\underline{\lambda}[\underline{Z}(\underline{X}^\circ)]$.

2. Using the initial set of trade-off ratios, maximize

$$H = \sum_{k=1}^{p} \lambda_k[\underline{Z}(\underline{X}^0)]Z_k(\underline{X})$$

This will give a new $\underline{X}^1$.

3. If $\underline{X}^1 = \underline{X}^0$, we know from Theorem I that it is optimum. If $\underline{X}^1 \neq \underline{X}^0$, have the decision maker evaluate a new set of trade-off ratios, $\underline{\lambda}[\underline{Z}(\underline{X}^1)]$, and repeat the same process until $\underline{X}^n = \underline{X}^{n-1}$.

It appears that Theorem I and the algorithm (perhaps in a modified form) would provide a useful addition/extension to the methodology presented in Section 2. In particular, it could be applied to the set of noninferior outcome

space. The facts that (1) we only have to consider a much smaller outcome space of noninferior solutions and (2) a full exposition of the problem will facilitate the assessment of the trade-off ratios (λ_k's) by the decision maker, should accelerate the convergence of the algorithm.

It would be very valuable to follow up more recent developments of Boyd's decomposition approach and its application to real problems.

C.3 Approach of Using Certainty Equivalents

It is mentioned that one could have reservations on the use of expected values as the sole measure of performance in the presence of uncertainties. This section discusses implications of the use of expected values and certainty equivalents. The use of expected values as measures of performance has implications about the underlying preference structures of the decision maker.

C.3.1 Outcome Space: Certainty versus Uncertainty

In Section 2.4, while trying to formulate our problem in analytical terms, it was assumed that each specific alternative we face--in the form of a vector of the decision variables $\underline{x}$--is associated with a unique set of consequences measured by the outcome vector $\underline{z} = (z_1,z_2,z_3,z_4)$ where the z_i's correspond to the expected frequency of core damage, expected acute fatalities, expected latent fatalities, and expected cost. This abstraction is certainly valid but it is, nevertheless, a summary description of the outcome of the realization of a particular alternative $\underline{x}$, that is, of building a nuclear power plant having safety systems characterized by the particular levels of unavailabilities (x_i's). Actually building such a plant means that a particular cost will be incurred and over its lifetime it is possible that an accident could happen which would result in a core damage and possibly in health effects that can be measured by acute and latent fatalities. Three of the four attributes can be measured easily in scalar quantities, namely, cost in dollars, acute and latent fatalities in number of deaths. The event of having a core damage can be also measured by a binary variable that takes the value of unity if the event actually happens and zero if it does not.

Having built a particular plant--having chosen a particular alternative $\underline{x}$--then, at the end of lifetime we would be able to measure the performance of the plant in our evaluation indices by four numbers:

z_1 (1 or 0 depending on whether a core damage occurred)

z_2 (number of acute fatalities)

z_3 (number of latent fatalities)

z_4 (incurred cost)

At the moment when the decision of choosing this alternative is being made, however, the exact value of these variables is not known. They are characterized by uncertainty. Each variable can actually take a value from a range of values. The only statement we can make a priori about the outcome of our decision has to do with the relative likelihood with which each possible quadruple of values (z^1,z^2,z^3,z^4) will occur. Consequently, to each possible

alternative $\underline{x}$ we cannot associate a single vector $\underline{\tilde{z}}$ but rather a random vector $\underline{z}$ and its associated probabilities, that is a multivariate probability density function. Given a specific plant configuration and unavailability levels $\underline{x}$, the PRA model for the plant yields the joint probability distribution $W(\underline{\tilde{z}})$ on the set of the outcome variables. The distribution can be generalized to include the uncertainties associated with the outcome of a specific alternative $\underline{x}$ and the uncertainties associated of the values of certain parameters, as well as a certain degree of incompleteness of the PRA model.

In conclusion, we can say that there is uncertainty associated with the outcome space of our problem and that what the PRA models do is to associate to each specific alternative (decision vector $\underline{x}$) a joint distribution function $W(\underline{\tilde{z}})$ over the outcome space R_0 (see sections 2.4 and A.3).

C.3.2 Preference Assessment under Uncertainty - Utility Theory

In the presence of uncertainty the comparison between two alternatives is more involved than in the case of certainty. Now given two alternatives $\underline{x}'$ and $\underline{x}''$ we have to compare not two points in the outcome space $\underline{z}'$ and $\underline{z}''$ but rather two random variables $\underline{\tilde{z}}'$ and $\underline{\tilde{z}}''$ characterized by the distribution

$$W'(\underline{\tilde{z}}') \text{ for } \underline{x}' \text{ and } W''(\underline{\tilde{z}}'') \text{ for } \underline{x}''. \qquad (C.1)$$

Utility theory provides a prescriptive way for making choices (assessing preferences) under uncertainty. The principles of utility theory are developed in Ref. 13. The essence of utility theory is that preferences under uncertainty are quantified by assessing a scalar utility function $u(\underline{\tilde{z}})=u(\tilde{z}_1,\tilde{z}_2,\ldots,\tilde{z}_n)$ over the outcome space of the n attributes. The utility function u has the characteristic property that, given two probability distributions A and B over the multiattribute consequences $\underline{\tilde{z}}$, probability distribution A is at least as desirable as B if and only if

$$E_A[u(\underline{\tilde{z}})] > E_B[u(\underline{\tilde{z}})] \qquad (C.2)$$

where E_A and E_B are the expectation operators taken with respect to distribution measures A and B, respectively. This asserts that expected utility is the appropriate criterion to use in choosing among alternatives. As a special degenerate case of (C.2) we conclude that outcome $\underline{z}'$ is at least as $\underline{z}''$ if and only if

$$u(\underline{z}') \geq u(\underline{z}'') \qquad (C.3)$$

Going back to our problem, if a utility function $u(\underline{\tilde{z}}) = u(\tilde{z}_1,\tilde{z}_2,\tilde{z}_3,\tilde{z}_4)$ has been defined on the outcome space R_0, then alternative $\underline{x}'$ is at least as preferred as $\underline{x}''$ if and only if

$$E_{W'}[u(\underline{\tilde{z}}')] \geq E_{W''}[u(\underline{\tilde{z}}'') \qquad (C.4)$$

where the expectation E_W has been taken over the measure W.

C.3.3 Certainty Equivalents

The definition of a utility function provided us with a way of comparing between two alternatives when their outcomes are characterized by uncertainty. Nevertheless, the joint distribution $W(\tilde{z})$ associated with each alternative $\underline{x}$ does not characterize the alternative in a convenient way. People think and understand single values better than distributions. The concept of certainty equivalent helps in reducing the distributions to single values.

Given a joint probability distribution A over the multiattribute consequence $\tilde{\underline{z}}$, a certainty equivalent of $\tilde{\underline{z}}$ is a point $\hat{\underline{z}}$ which in the opinion of the decision maker is equivalent to the uncertain option of the distribution A. From the definition of the utility function it follows that $\hat{\underline{z}}$ is the solution of the equation.

$$u(\hat{\underline{z}}) = E_A[u(\tilde{\underline{z}})] \tag{C.5}$$

where the expectation E_A is taken over the joint measure of $\tilde{\underline{z}}$. Eq. (C.5) defines an iso-utility curve in the space of $\underline{z}$. Any point $\underline{z}$ on this curve is a certainty equivalent. In the remainder of this section we will refer to the "certainty equivalent" when we actually mean a point of the iso-utility curve defined by Eq. (C.5).

Since the PRA model associates to each alternative $\underline{x}$ a distribution $W(\tilde{\underline{z}})$ over the outcome space R_0, if a utility function were available we could assign to each alternative $\underline{x}$ a vector $\hat{\underline{z}}$, i.e., the certainty equivalent where

$$u(\hat{\underline{z}}) = E_W[u(\tilde{\underline{z}})] \tag{C.6}$$

In this way, we can associate the decision space F_d (see Section 2.3, Figure 2.4) with a certainty equivalent outcome space R_0 through Eq. (C.6). Since this correspondence is not associated with uncertainty anymore, the general framework of the proposed methodology is also valid if we work with certainty equivalents in the outcome space (see Section A.5 for the use of mean values).

C.3.4 The Decomposition Principle--Use of Expected Values

The definition of certainty equivalents $\hat{\underline{z}}$ requires the prior knowledge of the multiattribute utility function $u(\underline{z})$. The assessment of such a function is, however, an involved and difficult task. Furthermore, if such a function is assessed, the establishment of the "noninferior" set of solutions (see Section A.3.3) is not necessary anymore, since the most preferred solution $\underline{x}^\circ$ could be determined by solving the single-objective optimization problem

$$\underline{x}^\circ \ni \min \; E_W[u(\tilde{\underline{z}})]. \tag{C.7}$$

The solution of this problem could, however, be a very difficult task. In situations like that, it could still be useful to replace the joint distribution over $\tilde{z}$, associated with each $\underline{x}$, with a certainty equivalent $\hat{z}$

determined from Eq. (C.6). Then, the methodology described in Subsections 2.4 and A.3 would provide a set of "noninferior" solutions in the space of certainty equivalents. Comparison among the elements of this set is now straightforward since to each solution ($\underline{x}^\circ$) corresponds a utility index $u(\underline{z}^\circ)$. For communication purposes, however, it would be much more preferable to display the noninferior solutions in terms of certain values (certainty equivalents) rather than in terms of distributions. This way, the effects of the utility function on the choice of the most preferred solution will be demonstrated in a clearer way. There are instances, however, where the certainty equivalents can be easily assessed. These cases are formally described in the following theorem.[13]

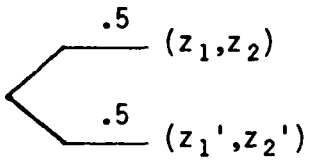
Theorem: The certainty equivalent $\hat{\underline{z}}$ for an uncertain alternative $\tilde{\underline{z}}$ is given by

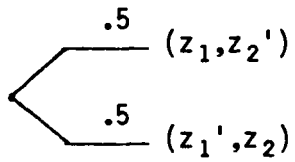
$$\hat{\underline{z}} = (\hat{z}_1, \hat{z}_2, \ldots, \hat{z}_n) \qquad (C.8)$$

where $\hat{z}_i$ $(i=1,2,\ldots,n)$ is the certainty equivalent for the one-dimensional variable $\tilde{z}_i$, calculated using the marginal distribution on z_i, provided that the attributes z_i are additive independent.

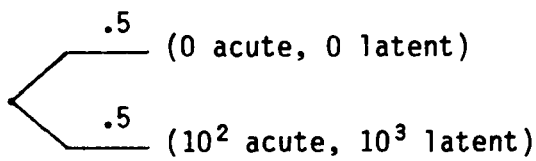
Definition: Attributes z_1 and z_2 are additive independent if the paired preference comparison of any two uncertain alternatives defined by two joint probability distributions on $Z_1 x Z_2$ depends only on their marginal probability distributions.

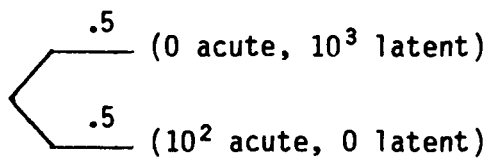
In two dimensions, an equivalent statement for additive independence is that the two lotteries





must be equally preferable for all (z_1,z_2) given an arbitrarily chosen z_1' and z_2'. Note that in each of these two lotteries, there is a one-half probability of getting either z_1 or z_1' and a one-half probability of getting either z_2 or z_2'. The only difference is how the levels of z_1 and z_2 are combined. Specializing this property to the attributes of acute and latent fatalities we have that if these two attributes are additive independent then the two lotteries





must be equally preferable. This of course is not automatically true.

One might argue that if there is an accident with 10^2 acute fatalities the addition of latent fatalities is overshadowed by the impact of the 10^2

acute deaths. Then, outcomes (10^2 acute, 10^3 latent) and (10^2 acute, 0 latent) have almost similar utilities or that the difference in their values is not the same as the difference between the outcomes (0 acute, 10^3 latent) and (0 acute, 0 latent). That is, the difference of 10^3 latent fatalities is more important at the zero level of acute fatalities than it is at the 10^2 level of acute fatalities.

If, nevertheless, the attributes are additive independent, then we can define the certainty equivalent $\underline{\hat{z}}$ of an uncertain outcome as follows. First, four one-dimensional utility functions $u_i(\tilde{z}_i)$ (i = 1,2,3,4) are assessed. This is a much easier task than assessing a multiattribute utility function $u(\tilde{z}_1,\tilde{z}_2,\tilde{z}_3,\tilde{z}_4)$. Next, for each alternative $\underline{x}$ the four certainty equivalents $\hat{z}_i$ (i=1,2,3,4) are assessed using the appropriate marginal probability distributions $W_i(\tilde{z}_i)$ which are provided by the PRA model. In this manner, the uncertainty outcome of each alternative is replaced by a certain outcome; namely $\underline{\hat{z}} = (\hat{z}_1,\hat{z}_2,\hat{z}_3,\hat{z}_4)$. The methodology described in Sections 2.4 and A.3 can now be applied. The set of noninferior solutions is now defined over the certainty equivalents. A value tradeoff among the various attributes (preference assessment) is still required as a final step. This preference assessment can be made, however, under certainty among the certainty equivalents. This simplification is possible because of the decomposition of the uncertainty problem into four single value uncertainty preference assessments, and it is valid only if the property of additive independence is valid for the four attributes.

If it is further assumed that the utility functions for each attribute are linear, that is

$$u_i(z_i) = z_i, \tag{C.9}$$

then the certainty equivalent is equal to the expected value of the variable since

$$E_W[u_i(z_i)] = E_W[z_i] = \bar{z}_i \tag{C.10}$$

and by virtue of (C.9) it follows that

$$\hat{z}_i = \bar{z}_i . \tag{C.11}$$

The assumption of linear utility functions is implied by any form of "safety goals" expressed in expected (mean) values. The existence of linear utility functions for each attribute is not, however, necessary for the validity of the proposed methodology. Any (assessed) form of single-value utility functions $u_i(\tilde{z}_i)$ can be incorporated into the PRA model to provide certainty equivalents.

APPENDIX D

UNCERTAINTY ANALYSIS

D.1 Introduction

It is recalled that the methodology we developed and applied to a relatively complex system was based upon three elements, i.e., (1) a plant PRA model, (2) reliability cost functions, and (3) (flexible) top level or global risk indices. The first two elements above are computational models for global risk measures and cost, respectively. These global measures are calculated (estimated) by synthesizing lower level reliabilities and costs.

As it was discussed in Section C.3, the outcomes of each specific alternative (i.e., the values of the global risk indices) are characterized by uncertainties. In Section C.3 a general approach to handling uncertainties through the certainty equivalents was presented. It was noticed, however, that the usefulness of the certainty equivalents required the strong assumption of additive independence on the decision maker's preference structure. In this section, we present a number of alternative approaches to the uncertainty problem, which do not require any knowledge about the decision maker's preference structure.

In Appendix A, we specified all the values of the outcome (global) variables, decision variables, and "state" variables that we dealt with as point values (means or certainty equivalents)*. A "state" variable is a variable which is not under control or not subject to decision, e.g., the elements of the site matrix and the initiator frequencies, the coefficients in the cost models, and in the case of the base model the elements of the containment matrix. It is noted here that the initiator frequencies could be additional decision variables in an extended allocation model. However, some of the elements of the site matrix could not be decision variables once the reactor site is decided (conceivably parameters referring to offsite protective action policies could be treated as decision variables).

The state variables of the model are, however, characterized by uncertainties themselves. Now, if the state variables $\underline{S}$ are uncertain (random variables), the same is true for the outcome variables $\underline{Z}$. We can state, then, the mathematical problem as a multiobjective optimization problem with uncertain state variables. A number of approaches to this problem are briefly described in the remainder of this section, under a variety of conditions. One of the approaches is applied to the base model used in the main report.

D.2 Approaches

Following the "separation" of the decision variables from state variables as discussed in the previous section, the allocation problem in a multiobjective programming formulation is expressed as

*It was shown in Section C.3 that the certainty equivalents become equal to the means under the assumptions of additive independence and linearity of the utility function.

$$(P_0) \quad \underset{\underline{X}}{\text{Minimize}} \ \underline{Z}(\underline{X}, \underline{S}) = [C_d(\underline{X}, \underline{S}), A(\underline{X}, \underline{S}), L(\underline{X}, \underline{S}), G(\underline{X}, \underline{S})]$$

where $\underline{X}$ is the vector of decision variables as before and $\underline{S}$ the vector of uncertain state variables.

Recall that in Section A.3.3.1 minimization of a vector $\underline{Z}$ means finding noninferior solutions.

D.2.1 Allocation Under Uncertainty

The approaches which belong to this class consider uncertainties before the optimization problem is solved. Thus the uncertainties are imbedded formally in the allocation procedure.

D.2.1.1 Brute-force (Monte Carlo Sampling) Approach

$$(P_1) \quad \underset{\underline{X}}{\text{Minimize}} \ \underset{\underline{S}}{\text{Sample}} \ \underline{Z}(\underline{X},\underline{S})$$

where the distributions of $\underline{S}$ are given. The Monte Carlo sampling is straightforward when the s_i's are statistically independent or completely dependent. There also exist Monte Carlo sampling techniques for handling the cases when the s_i's are dependent and distributed according to a joint distribution function. Implementation of these techniques is, however, rather involved.

Since this approach requires one (vector) minimization problem be solved for each realization of the Monte Carlo sampling, the overall computational effort will be highly demanding for reasonable sampling accuracy.

D.2.1.2 α-Confidence Level Approach

Assumptions for this approach are the following:

i) The global attributes are linear in $\underline{S}$, e.g., only the site matrix and the coefficients in the reliability cost models are uncertain and all the other parameters are either decision variables or constant.

ii) Variance of each uncertain variable s_i and, if some of uncertain variables are correlated, Cov (s_i,s_j) are given.

iii) The uncertain variables are normally (or truncated normally) distributed.

Recall the constraint method we can use to solve the multiobjective optimization problem (P_0), i.e.,

$$(P_2) \quad \underset{\underline{X}}{\text{Minimize}} \ C_d(\underline{X})$$

$$\text{subject to } \underline{X} \in F_d$$

$$A(\underline{X},\underline{S}) \leq \varepsilon 1$$

$$L(\underline{X},\underline{S}) \leq \varepsilon_2$$

$$G(\underline{X},\underline{S}) \leq \varepsilon_3.$$

We now seek the noninferior solution set at the α-confidence level, parametrically in α. Here α is the minimum probability of achieving the constraints on A, L, and G, that is,

(P_2') Minimize $C_d(\underline{X})$
$\underline{X}$

subject to $\underline{X} \in F_d$

$$P_r[A(\underline{X},\underline{S}) \leq \varepsilon_1] \geq \alpha$$

$$P_r[L(\underline{X},\underline{S}) \leq \varepsilon_2] \geq \alpha$$

$$P_r[G(\underline{X},\underline{S}) \leq \varepsilon_3] \geq \alpha.$$

Under the stated assumptions, using the concept of deterministic equivalents, (P_2') can be transformed into:

(P_2'') Minimize $C_d(\underline{X})$
$\underline{X}$

subject to $\underline{X} \in F_d$

$$A(\underline{X},\overline{\underline{S}}) + K_\alpha[A_X^T B A_X]^{1/2} \leq \varepsilon_1$$

$$L(\underline{X},\overline{\underline{S}}) + K_\alpha[L_X^T B L_X]^{1/2} \leq \varepsilon_2$$

$$G(\underline{X},\overline{\underline{S}}) + K_\alpha[G_X^T B G_X]^{1/2} \leq \varepsilon_3$$

where K_α is a standard normal value such that $\Phi(K_\alpha) = \alpha$ and Φ represents the cumulative standard normal distribution, and B is a symmetric variance-covariance matrix of the uncertain variables. $\overline{\underline{S}}$ stands for the mean of $\underline{S}$, and A_X for $\underline{f}\ \underline{M}(\underline{X})\ \underline{C}$ (similarly L_X and G_X are appropriately defined functions of $\underline{X}$).

It is noted in (P_2'') that when $\alpha = 0.5$ K_α becomes zero and (P_2'') reduces to the problem we solved in Appendix B and that the second terms in the constraints are perturbations to the first terms, reflecting the effects of uncertainties in $\underline{S}$ on A, L, and G.

Operationally, (P_2'') would be solved as follows:

i) Choose a specific α from a discrete set of α's (e.g., α =0.1,0.2, ...,0.9).

ii) Solve the multiobjective problem (P_2") by varying the ε_i's as we did in Appendix B.

iii) Go to i).

It is noted that this approach allows for incorporation of the uncertainties in the allocation procedure by solving only several deterministic (not stochastic) problems. This is of course possible under the stated assumptions.

The solutions would look like Fig. D.1 in a two-dimensional example. The noninferior solutions would be displayed at several confidence levels.

D.2.2 Uncertainty on Allocation

In these approaches we do not consider uncertainties before allocation but first solve the allocation problem using mean values and then examine the variation of global attributes due to uncertainties of the state and/or decision variables.

D.2.2.1 Uncertainty Propagation Approach

The variation of global attributes can be examined by using the various uncertainty propagation methods[23], e.g., response surface technique, method of moments, and Monte Carlo sampling. Two approaches using the Monte Carlo sampling technique are the following:

(P_3) i) $\underset{\underline{X}}{\text{Minimize}}\ \underline{Z}(\underline{X},\underline{\bar{S}})$

ii) $\underset{\underline{S}}{\text{Sample}}\ \underline{Z}^*(\underline{X}^*,\underline{S})$

where $\underline{Z}^*$ and $\underline{X}^*$ are the noninferior solutions from i).

(P_4) i) $\underset{\underline{X}}{\text{Minimize}}\ \underline{Z}(\underline{X},\underline{\bar{S}})$

ii) $\underset{\underline{X},\underline{S}}{\text{Sample}}\ \underline{Z}^*(\underline{X}^*,\underline{S})$

where $\underline{Z}^*$ and $\underline{X}^*$ are the noninferior solutions from i).

D.2.2.2 Mean-Variance Approach

Assumptions for this approach are the same with the first two assumptions i) and ii) for the α-confidence level approach.

(P_5) i) Minimize $\underset{\underline{X}}{\underline{Z}}(\underline{X},\underline{\bar{S}})$

ii) Calculate Var $\underline{Z}^*(\underline{X}^*,\underline{S})$
$\underline{S}$

where $\underline{Z}^*$ and $\underline{X}^*$ are the noninferior solutions from i).

D.3 Example

As an example of uncertainty analysis, the uncertainty propagation approach (P_4) described above is applied to the base allocation model used in the main report. The approach (P_4) first solves the allocation problem using mean values and then propagate uncertainties of the state and decision variables through the model by using the Monte Carlo sampling techniques.

Tables D.1 through D.4 show the input data used in the uncertainty analysis, and Table D.5 and Figs. D.2 through D.5 provide the results. A modified version (to handle multiple outputs in a single run) of the SAMPLE program in WASH-1400 was used assuming all uncertain variables follow the lognormal distributions with appropriate mean values and error factors.

It is noted from Figs. D.2 through D.5 that, if only one attribute is considered in isolation of the other attributes, the noninferior solution C8 stochastically dominates the noninferior solution B5 in the core damage frequency, acute fatalities and latent fatalities, while the noninferior solution B5 stochastically dominates the noninferior solution C8 in the reliability cost. Clearly, the attribute of reliability cost conflicts with the other three attributes in choosing one from the two alternatives B5 and C8. Thus, in this situation, choosing one alternative requires a decision maker's preference assessment. It may also happen that none of the alternatives exhibits stochastic dominance in any of the attributes if the alternatives are "close" enough. In any case, uncertainty analysis around the noninferior solutions should facilitate preference assessment of a decision maker because it reveals more relevant information about the problem.

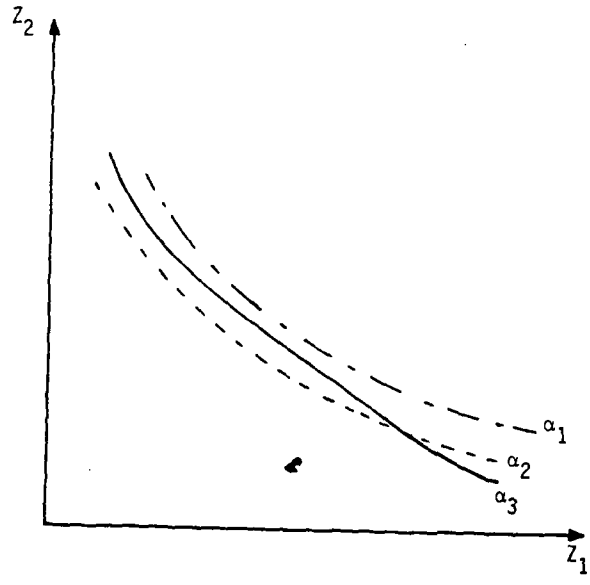


Figure D.1 Noninferior outcomes at several confidence levels.

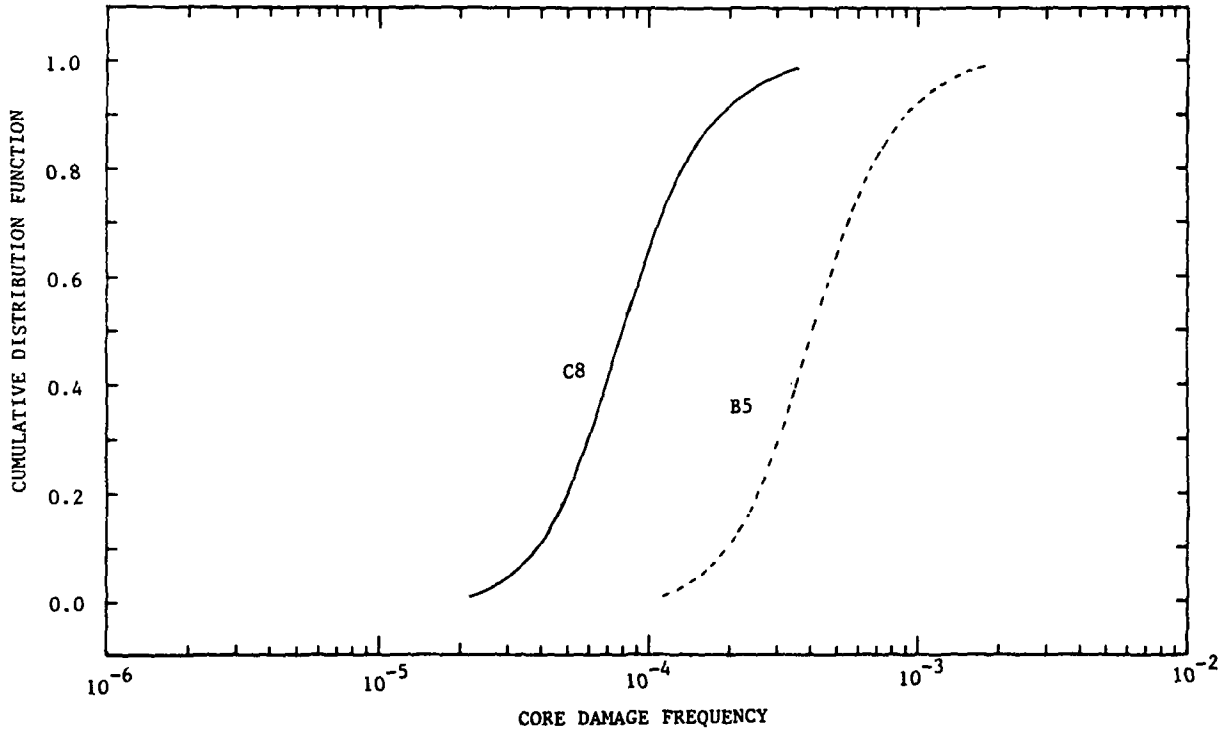


Figure D.2 Cumulative distribution of core damage frequency for noninferior solutions B5 and C8.

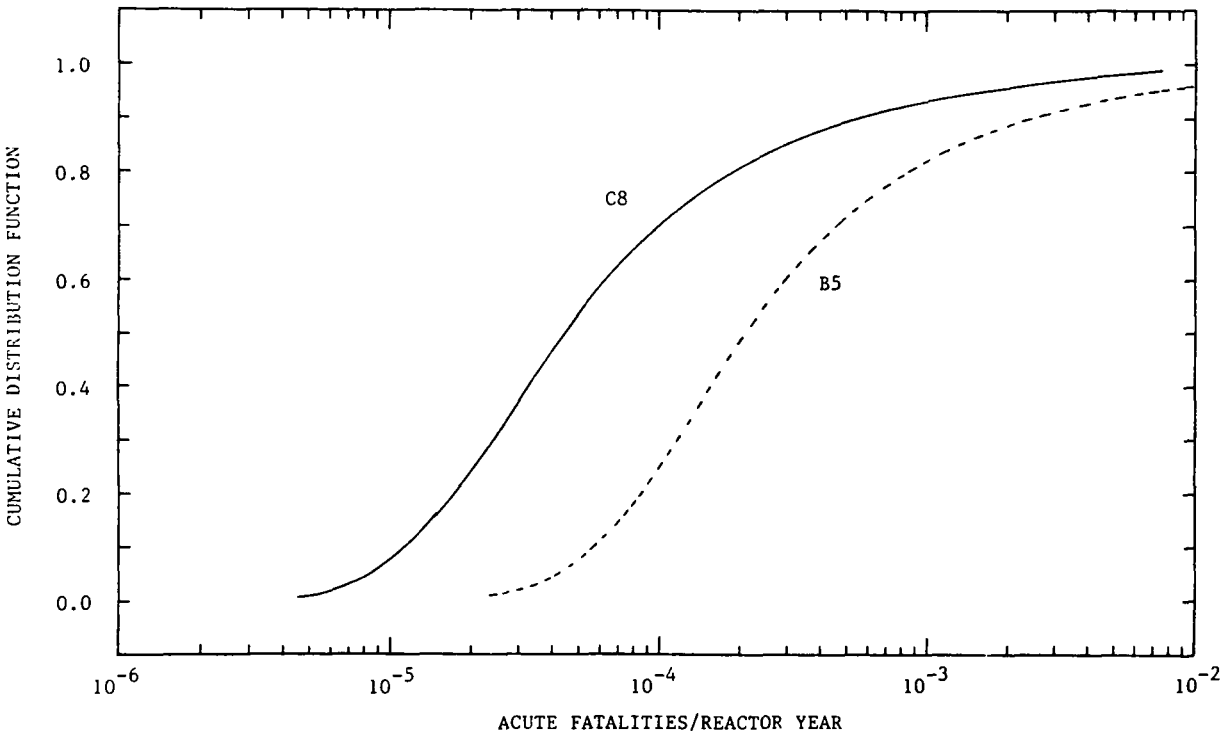


Figure D.3 Cumulative distribution of acute fatalities/reactor year for noninferior solutions B5 and C8.

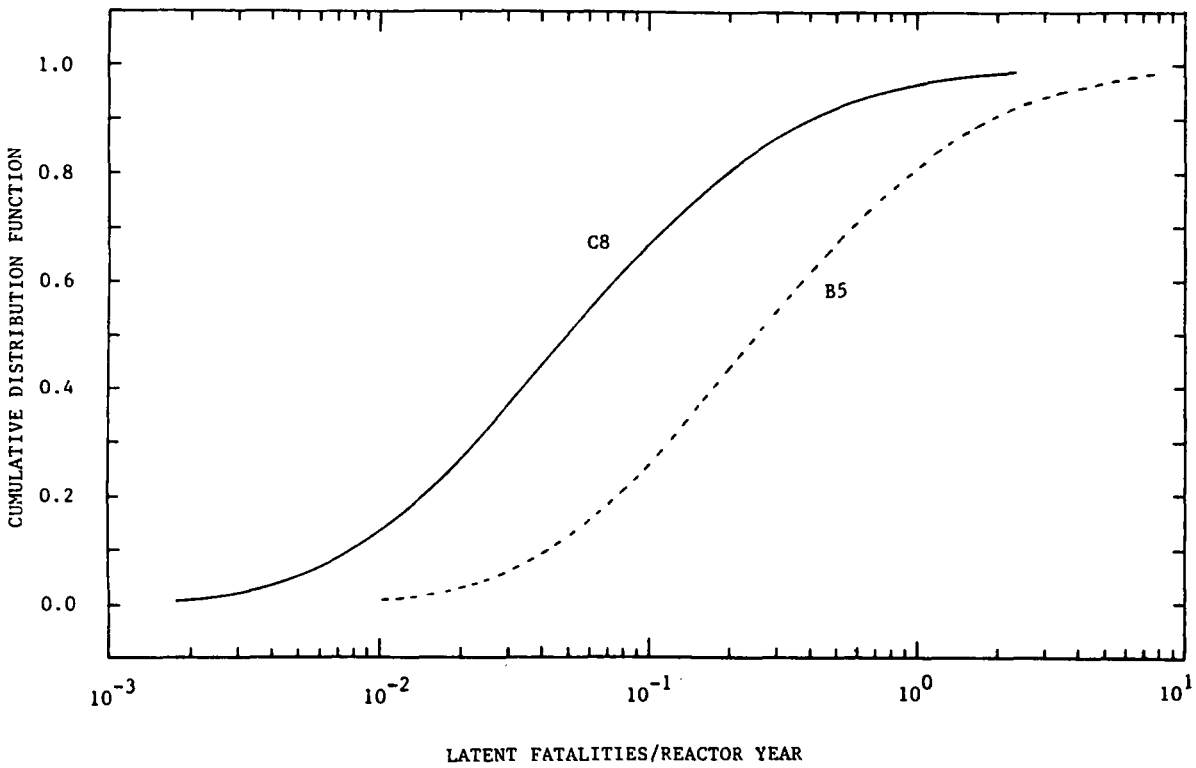


Figure D.4 Cumulative distribution of latent fatalities for noninferior solutions B5 and C8.

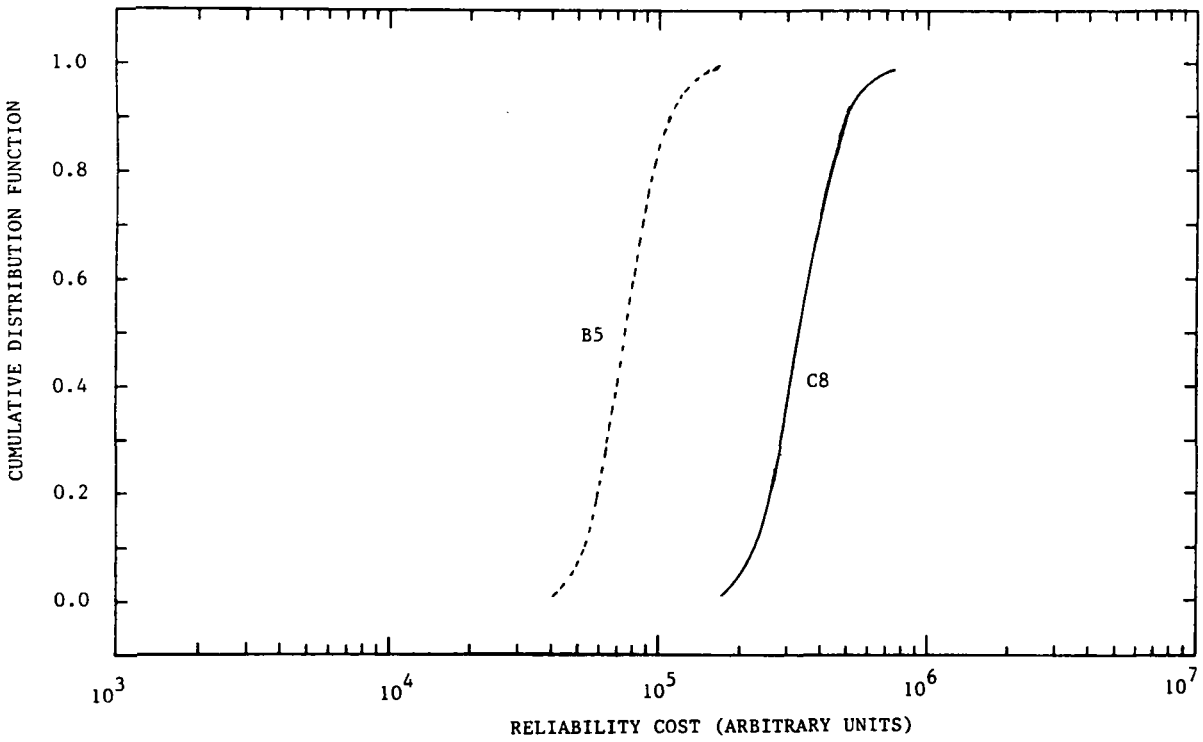


Figure D.5 Cumulative distribution of reliability cost for noninferior solutions B5 and C8.

Table D.1 Uncertainties in Initiator Frequencies

Initiator	Mean (Events/Reactor Year)	EF*
LOFW/MSIV Closure	1.23	2.3
LOSP	0.17	4.4
Turbine Trip	8.17	1.5

*90% error factor under the lognormal distribution in Ref. 4.

Table D.2 Uncertainties in Containment and Site Matrices*

Accident Class	α_i Mean**	EF***	β_i Mean**	EF***
I	2.132(-1)	2.8	1.709(+3)	23.5
II	4.277(-1)	2.1	1.381(+3)	16.3
III	2.132(-1)	2.8	1.709(+3)	23.5
IV	8.071(+1)	34.4	1.308(+4)	27.0

*α_i is the expected acute fatalities given Accident Class i and β_i is the expected latent fatalities given Accident Class i since $\underline{\alpha}\ \underline{\beta} = \underline{C}\ \underline{S}$.
**Best-estimate in Ref. 4.
***90% error factor assuming the lognormal distribution.

Table D.3 Uncertainties in α_i of Reliability Cost Functions Assumed in Uncertainty Analysis

	Component	Mean	EF*
1.	RPS(M)	10.	3
2.	SLCSH	1.	3
3.	LOSP	1.	5
4.	EDC	1.	2
5.	WSW	1.	3
6.	FWPCS	10.	5
7.	ARC	1.	3
8.	RCICH	1.	3
9.	HPSIH	1.	3
10.	ADSH	1.	5
11.	LPCIH	1.	3
12.	LPCSH	1.	3
13.	RECOV	10.	2
14.	RHRH	10.	3
15.	FWPCSL	10.	3
16.	DG	10.	10
17.	X	1.	2
18.	D	1.	5
19.	FWPCSL(RECOV)	10.	2

*90% error factor assuming the lognormal distribution.

Table D.4 Uncertainties in Achieved Unavailabilities Assumed in Uncertainty Analysis for the Noninferior Solutions B5 and C8

	B5		C8	
	Mean*	EF**	Mean*	EF**
X(1)	1.65(-3)	3	3.66(-4)	3
X(2)	7.27(-4)	3	3.15(-4)	3
X(3)	5.20(-4)	5	5.20(-4)	5
X(4)	2.73(-5)	3	5.57(-6)	3
X(5)	6.10(-5)	5	1.25(-5)	5
X(6)	5.31(-3)	5	5.00(-3)	5
X(7)	1.50(-1)	3	1.50(-1)	3
X(8)	1.00(-2)	5	1.00(-2)	5
X(9)	1.00(-2)	5	1.00(-2)	5
X(10)	6.79(-3)	5	1.43(-3)	5
X(11)	3.75(-2)	5	1.31(-2)	5
X(12)	3.56(-2)	5	1.23(-2)	5
X(13)	5.00(-2)	10	5.00(-2)	10
X(14)	2.05(-3)	5	5.40(-4)	5
X(15)	3.52(-3)	5	1.40(-3)	5
X(16)	1.65(-3)	5	3.36(-4)	5
X(17)	7.44(-3)	10	1.43(-3)	10
X(18)	2.00(-3)	10	2.00(-3)	10
X(19)	5.00(-2)	5	5.00(-2)	5

*Noninterior solutions obtained from the base model.
**90% error factor assuming the lognormal distribution.

Table D.5 Cumulative Distributions* of Core Damage Frequency Acute Fatalities, Latent Fatalities, and Reliability Cost for the Noninferior Solutions B5 and C8

		5th Percentile	Median	95th Percentile	Mean
Core Damage Frequency	B5	1.57(-4)	4.08(-4)	1.15(-3)	5.00(-4)
	C8	3.10(-5)	8.13(-5)	2.32(-4)	1.00(-4)
Acute Fatalities	B5	4.19(-5)	2.08(-4)	7.35(-3)	2.56(-3)
	C8	8.24(-6)	4.32(-5)	1.63(-3)	5.65(-4)
Latent Fatalities	B5	2.51(-2)	2.53(-1)	3.50(+0)	1.17(+0)
	C8	4.71(-3)	5.03(-2)	7.32(-1)	2.46(-1)
Reliability Cost	B5	4.77(+4)	7.56(+4)	1.25(+5)	7.98(+4)
	C8	2.02(+5)	3.34(+5)	5.73(+5)	3.54(+5)

*Using Monte Carlo sampling size of 4800.

APPENDIX E

DISCRETE ALTERNATIVES AND A TWO-LEVEL DECOMPOSITION APPROACH TO DISCRETE MULTIOBJECTIVE OPTIMIZATION

When component reliabilities are allowed to take only discrete values or when there are only discrete alternatives, the reliability allocation methodology formulated in Appendix A becomes a discrete optimization (integer programming[24] problem with multiple objective functions.

The discrete optimization problems require fundamentally different mathematical techniques from those used in the continuous optimization problems. The decision variables in a discrete optimization problem, being discrete rather than continuous, forbid the use of "calculus of variations," but require combinatorial comparisons which become computationally intractable when the problem is large. The computational intractability becomes even more severe for the problem of finding noninferior configurations (the definition of noninferiority for a discrete problem is similar to that for a continuous problem in Section A.3.3), since in this case the solution process entails exhaustive pairwise comparisons of vectors; vectors here being composed of multiple objective functions. Thus, even the intrinsically discrete problems are usually approximated by continuous problems first and then the techniques for the continuous problems are used.

The two-level decomposition approach to be discussed in this appendix is a combinatorial approach but avoids the exhaustive comparisons. It requires only partial comparisons and thus is efficient. It is based on the traditional idea of "divide and conquer."

In the two-level decomposition approach, as depicted in Figure E.1 in a two-dimensional case, the search of noninferior configurations is performed at two levels. The decision space of all alternative configurations is first divided into several subspaces, and noninferior configurations are determined for each subspace. The final noninferior configurations are then determined for the union of noninferior configurations found from the first level.

The efficiency of this approach was tested in an example problem which is known as redundancy optimization in the reliability literature[25]: finding noninferior configurations of a system which consists of 5 stages and in which each stage is allowed to have up to 5 redundant components (see Figure E.2). The multiobjective functions were the system unreliability and the system cost. (The system weight and volume could also have been included.) The total number of alternative configurations was 3125. The first-level decomposition found 422 noninferior configurations which were subsequently reduced in the second-level decomposition to 60 noninferior configurations. The total number of pairwise vector comparisons was $\sim 1.3 \times 10^5$ which is smaller by a factor of 5 than that of no decomposition (which required $\sim 6.5 \times 10^5$ pairwise vector comparisons). Thus, the decomposition approach is efficient.

Table E.1 shows the component unreliabilities and costs used in the example. Figure E.3 shows the noninferior configurations found from the two levels. The 422 noninferior configurations found from the first level are represented by x's and the 60 noninferior configurations from the second level

are connected by solid lines in the figure. As an illustration, Table E.2 shows information about the redundancy at each stage, system unreliability, and system cost for three noninferior configurations.

It is noteworthy that the noninferior cost-unreliability curves determined by the two-level decomposition approach could be used as reliability cost functions for "supercomponents" employed in Appendix B.

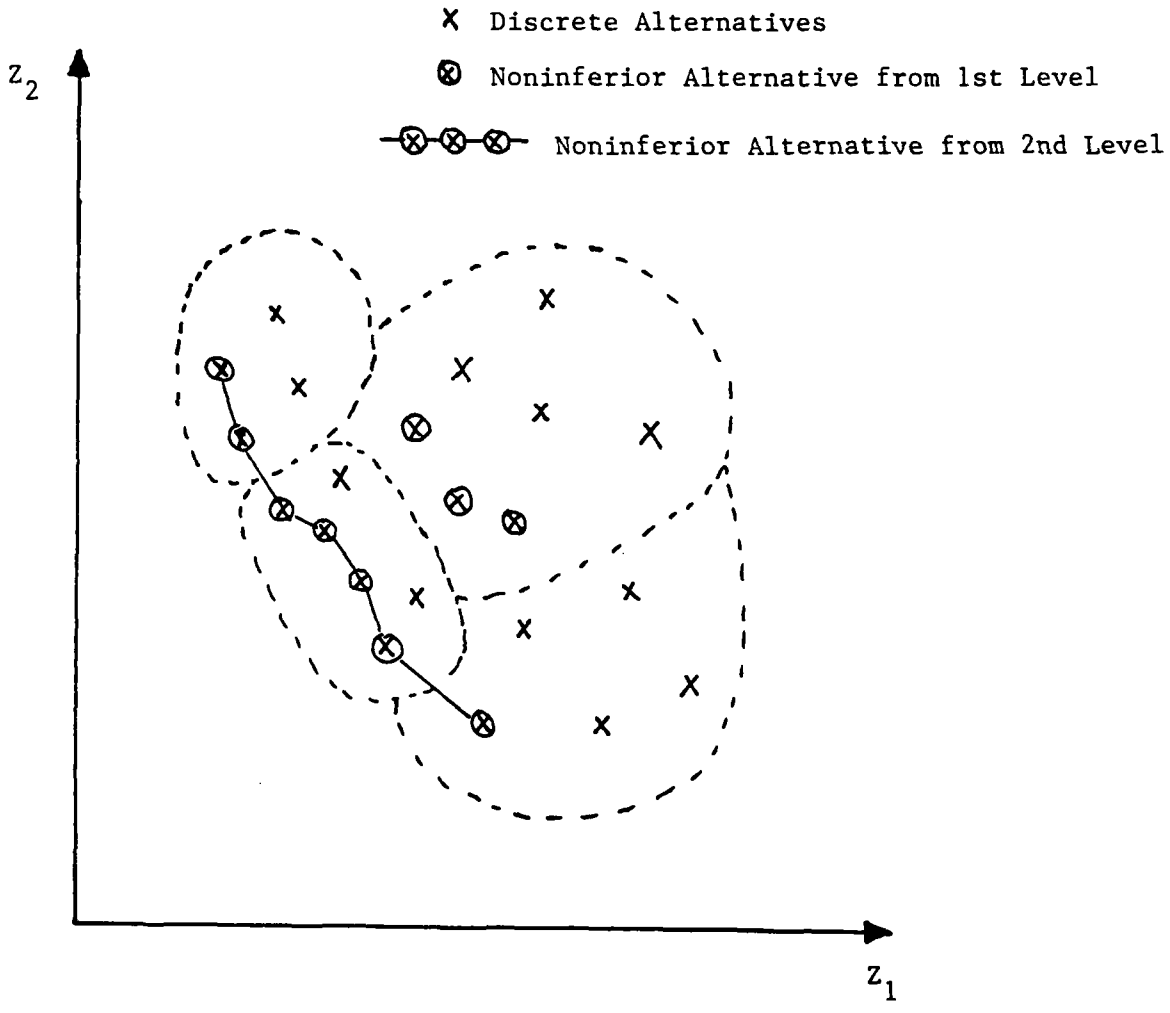


Figure E.1 Two-level decomposition approach to discrete multiobjective optimization.

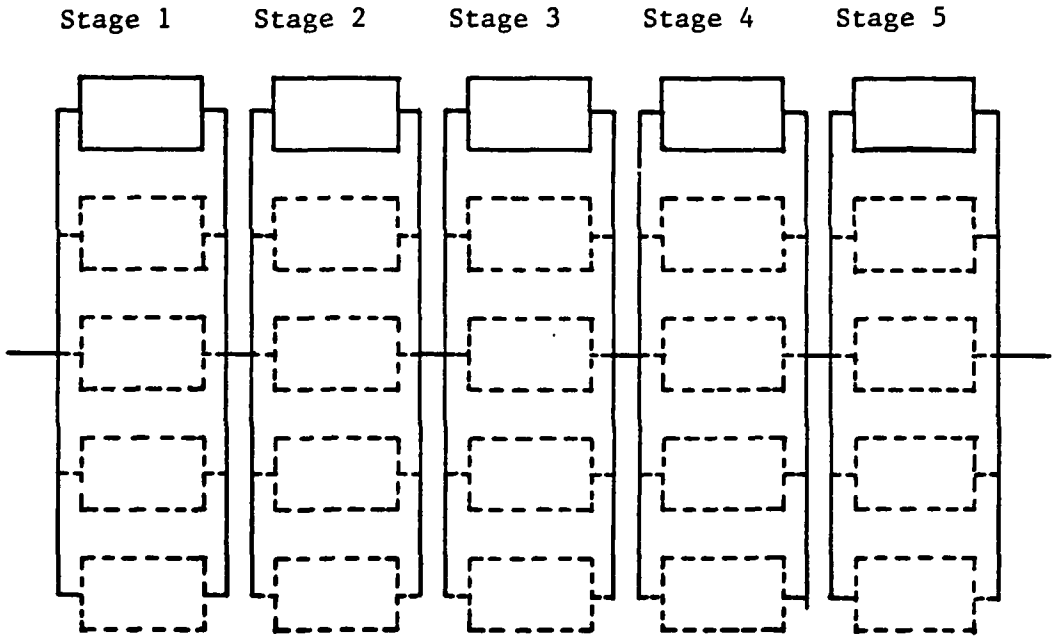


Figure E.2 Example problem for redundancy optimization.

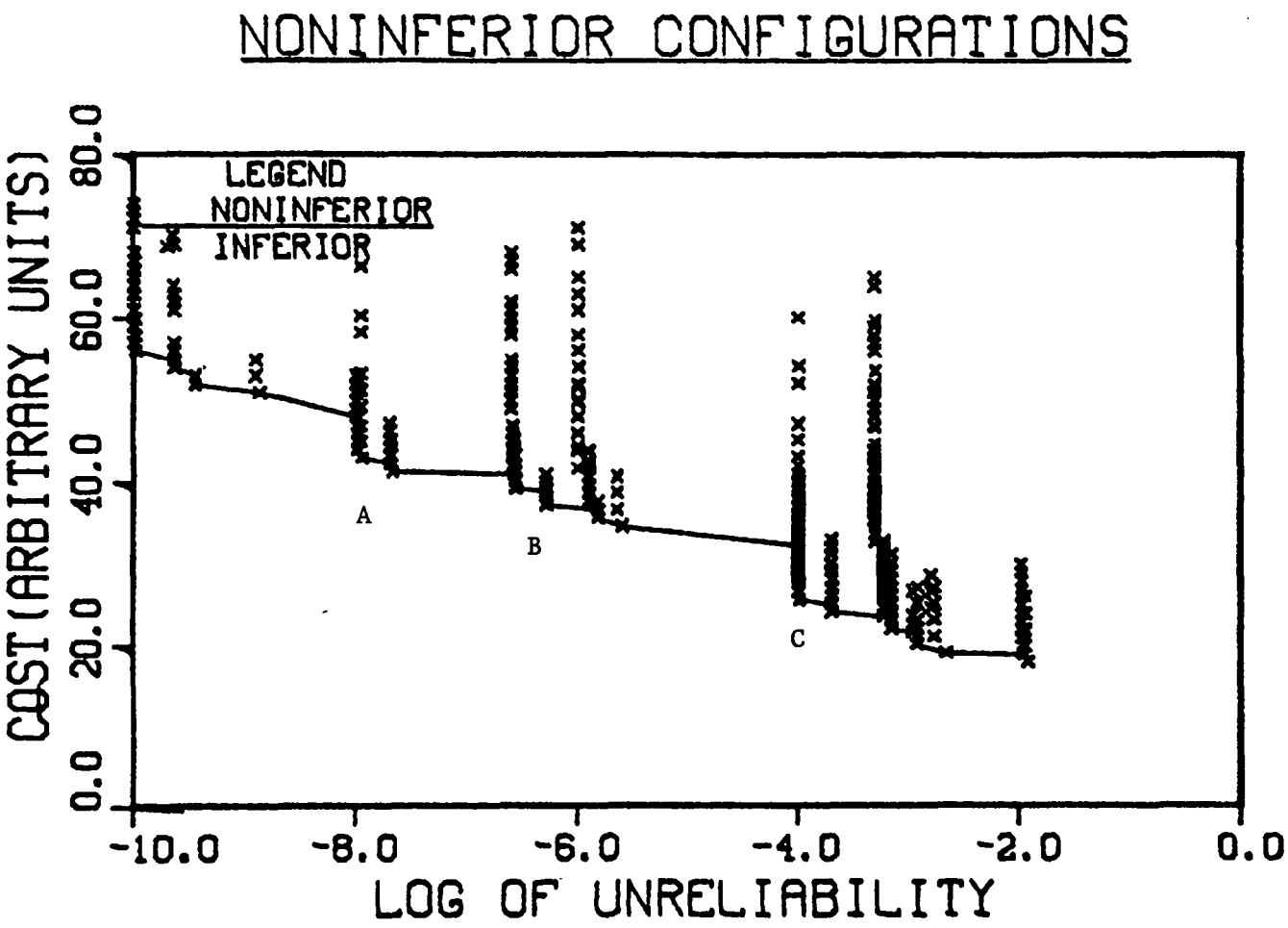


Figure E.3 Noninferior configurations of the example problem found by the two-level decomposition approach.

APPENDIX F

COMMENTS FROM THE MEMBERS OF THE STEERING GROUP AND DISCUSSIONS FROM THE AUTHORS

F.1 Steering Group Members

Dr. George W. Cunningham
Director of Technology Studies
The MITRE Corporation
1820 Dolley Madison Boulevard
McClean, VA 22102

Dr. B. John Garrick
Pickard, Lowe, and Garrick, Inc.
2260 University Drive
Newport Beach, CA 92660

Prof. Elias P. Gyftopoulos
Ford Professor of Nuclear Engineering
Department of Nuclear Engineering
Massachusetts Institute of Technology
Cambridge, MA 02139

Prof. Ronald A. Howard
(Stanford University)
Strategic Decisions Group
3000 Sand Hill Road
Menlo Park, CA 94025

Mr. F. Stanley Nowlan
(Retired--United Airlines, Director of Maintenance Analysis)
Consultant
P.O. Box 1381
Sausalito, CA 94966

F.2 Questions for the Steering Group

The following list of specific questions was sent to each member of the Steering Group along with our first interim report dated January 1984:

1. Are the objectives of this program well defined?

2. Are there any fundamental flaws with the methodology outlined by BNL?

3. Have there been attempts (successful or unsuccessful) to solve similar problems in other fields? What are the relevant lessons for this program?

4. Are there approaches or methodologies that may be useful in the BNL program which are currently being overlooked by BNL?

5. What is your view on the use and selection of "cost" models?

6. What are your views on the possibility of addressing this problem on a generic basis? In other words, is a plant specific PRA model always necessary?

7. Given that many of the model parameters are uncertain, how should this be reflected (or displayed) in the final results?

8. What are your views on the "Limitation and Problem Areas" as discussed in the first interim report?

F.3 Written Comments from the Steering Group Members*

F.3.1 Comments by George W. Cunningham

I am writing to give you a few comments on the steering group meeting held on 19 March 1984 at the NRC in Bethesda. I will follow up in a few weeks with some other thoughts--particularly with regard to the discussion on influence diagrams. First, as agreed in our meeting, I believe it is important that you continue with the present approach but that you try to calculate results with a specific example. While I would also agree that it will be interesting and enlightening to pursue the methodology proposed by Ron Howard, the work on methodology should not be allowed to overshadow the other objectives which you have outlined.

The question of setting safety goals remains a controversial issue. Nevertheless, it seems to me that your program should make a concerted effort to determine whether safety goals can be used as a basis for reliability allocation. At the same time the actual goals used should be critically examined as a part of the process. While a generic solution may be possible in the future it does not seem feasible at this time. There is a wide range in design of reactor as constructed, a wide range in individual plant reliability and performance, and a wide range in utility resources and qualifications. For your purposes a generic solution will be useful in terms of setting forth methodology but may not offer much help in terms of providing cost-benefit tradeoffs for changes in a particular plant.

The specific safety goals selected for this study tend to emphasize prevention of severe accident conditions. While this is a worthy goal, it seems that this approach would tend to place emphasis on reliability of containment and certain "safety related" systems. The point was made in the discussion that the core melt goal is driving the requirements for most plants. Thus there is a real danger that emphasis will be placed on reliability of infrequently used components and back up system and not on reliability of operating systems and components. A plant which is operating well and has a good capacity factor will be more likely to have a good safety record.

In response to your specific questions, I have the following comments:

*These comments were made on the first interim report and the first Steering Group meeting presentation held on March 19, 1984.

1. Are the objectives of this program well defined?

As I indicated at the steering group meeting the objectives are clearly expressed but may be overly ambitious. I believe your chances of success will be greater if you select as a "base" plant one for which there is a good quality PRA available and most important, one which has a good operating record and a high reliability. It seems to me that by eliminating as many uncertainties as possible prior to the analyses you will be in a better position to judge the real feasibility of reliability allocation.

2. Are there any fundamental flaws with the methodology outlined by BNL?

This issue was discussed at the steering group meeting and there seems to be general agreement that the mathematics are correct. My concern with the approach is more related to the "cost" model as discussed in question 5 and the potential that noninferior solutions may not exist or may exist locally but not globally.

3. Have there been attempts (successful or unsuccessful) to solve similar problems in other fields? What are the relevant lessons for this program?

The approach used by the FAA is more deterministic in nature but at the same time a set of broad criteria and design requirements have evolved over a period of time to create acceptable engineering practice. If the design can meet these criteria, there will be considerable leeway in designing the air frame while still meeting FAA requirements for an airworthiness certificate. The work by Stan Nowlan on reliability centered maintenance also has real potential for application in nuclear systems. The FAA system accepts certain levels of risk without establishing a safety goal per se, but the most important factor is the systems approach. The entire system is evaluated as an integrated system, not just a total of individual components which fail or don't fail. Thus the impact of one component failure on another is considered.

4. Are there approaches or methodologies that may be useful in the BNL program which are currently being overlooked by BNL?

As stated earlier, the approach by Ron Howard may be helpful. I will comment more on this in a follow-up letter.

5. What is your view on the use and selection of "cost" models?

While recognizing cost as an important factor, I don't believe that cost alone can serve as an optimization factor for systems which have met the criteria necessary to be within your calculated envelope. The necessity for redundant systems presupposes that reliability in that case is not adequate regardless of cost. On the other hand, it is well known that in many cases reliability can be greatly improved with little cost. The key question will revolve around costs vs benefits for any retrofit. Unfortunately it may be difficult to ascertain the uncertainties and to project future reliability in comparison with known reliabilities of the existing system. Nevertheless, the objective of accomplishing the safety goals at a minimum total cost remains valid.

6. What are your views on the possibility of addressing this problem on a generic basis? In other words, is a plant specific PRA model always necessary?

The question has been partially discussed in the body of this letter. It is likely that a plant specific PRA would be necessary in any event to check against conclusions obtained from a generic plant. However, it might be possible to use a generic PRA to provide guidance, and then utilize plant specific reliability data to determine modifications required.

7. Given that many of the model parameters are uncertain, how should this be reflected (or displayed) in the final results?

I would suggest that this question is premature and should be discussed at the next meeting.

8. What are your views on the "Limitation and Problem Areas" as discussed in the draft report?

This area needs to be expanded. Some concerns and examples of problems were expressed at the group meeting. Nevertheless it seems desirable to complete the calculation on a specific example prior to discussing this question any further.

I hope this letter will be helpful. Please call me if you have any questions.

F.3.2 Comments by B. John Garrick

The referenced paper does a nice job of exploring the ideas of optimal reliability allocation. It makes the point we have long promoted; namely, that one should not design based on safety goals alone. In the context of the BNL example of "decision variable space," designing to safety goals alone puts the outcomes on the boundary of the admissible space. The BNL paper properly points out that the damage functions are very complicated, the λ's uncertain, the cost functions not known, and the value judgments unmade. They thus support the important conclusion (though they do not draw it) that the whole allocation idea is infeasible.

BNL advocates something called multiobjective optimization which really means what we have been calling risk management. The BNL approach has one fundamental flaw however. They work backwards from the goals to the λ_i as if the λ_i were able to be arbitrarily chosen continuous variables. Our experience is that the better approach is to recognize that there are a finite number of design possibilities for any system, e.g.,

$$(\lambda_i)_1, (\lambda_i)_2, (\lambda_i)_3$$

each with a corresponding cost. The approach involves employing a "forward" or "decision theoretic" assembly process for each of the design options, determining the effect on all the risk/availability indices, and then choose which set of design probabilities is the best cost/risk/benefit tradeoff. The approach is logical, understandable, and feasible. Enclosed are three

papers plus some figures expanding on some of the points. The key issue is that the "how safe is safe enough" question is an unanswerable question because it is out of context and thus illogical. It is the real reason why the safety goals are not a feasible approach. If the safety goal concept is not changed, the nuclear industry has once again shot itself in the foot.

There are many other serious questions concerning the feasibility of reliability allocation. It all really depends on what is meant by reliability allocation criteria. If the desire is to allocate reliability requirements to equipment and components, then in addition to the problems associated with the single-objective approach there is the very serious problem of boundary conditions and dependencies. In particular, components and equipment are very sequence dependent which makes them very plant specific dependent. Thus any generic approach would run the high risk of being either too conservative or nonconservative and seldom just right. Again the better approach is believed to be to consider the options on a plant specific basis in a decision analysis framework. Of course, if we ever get to the point of standard plant designs, then some logical reliability criteria may evolve.

Turning to the questions to the Steering Group.

1. Are the objectives of this program well defined?

The objectives are well defined in view of the fact that they provide the freedom to deal with the "feasibility" issue. That is, the objectives do not preclude the conclusion that reliability allocation is logically unachievable.

2. Are there any fundamental flaws with the methodology outlined by BNL?

Yes, please see introductory remarks.

3. Have there been attempts (successful or unsuccessful) to solve similar problems in other fields? What are the relevant lessons for this program?

Reliability allocation is a topic discussed in many references in reliability; for example, see References 1, 2, and 3. Most of the have been made in defense programs where economics were a secondary consideration. In my research on this topic, I have seen many examples of application but cannot be convinced of its utility especially in the nuclear plant risk business where cost is important and system/component interdependencies play such a major role. If by reliability allocation we mean exposing the costs, risks, and benefits of the various options available to us, then it is a very good idea.

4. Are there approaches or methodologies that may be useful in the BNL program which are currently being overlooked by BNL?

It is expected that BNL has done a good job of researching available methods and applications. Their recognition of the illogical nature of single-objective programming is an important step forward.

5. What is your view on the use and selection of "cost" models?

The cost models are logical and general. Of course, real problem applications usually drive the details of a cost model. Since such examples are

not presented, it is too early to deal with what may be the most important point, namely, the interpretation of the cost components and the use of cost data.

6. What are your views on the possibility of addressing this problem on a generic basis? In other words, is a plant specific PRA model always necessary?

As a practitioner of PRA, it would of course be expected that I would be biased towards the need for plant specific PRAs. Nevertheless, the evidence continues to increase extensively in favor of the need for integrated plant specific models to intelligently make decisions about plant safety and operations. The closest thing to such models are the contemporary full scope risk assessments. Obviously, if there is an alternative approach, it should be considered. The absence of standardized plant designs makes generic approaches extremely limited in value. This fact along with the component interdependencies gives me little hope that generic reliability allocation can serve much value except to continue the process of driving up the cost of electric power. For example, in the Seabrook PRA almost 60% of the core melt frequency came from dependent initiating events. Since all the plants are different and each has three to four million components, if I were a utility decision-maker, I would insist on my own risk model. I just do not think we can get there without them. An integrated plant specific model is a small price to pay to nail down the role of specific components, procedures, and actions.

7. Given that many of the model parameters are uncertain, how should this be reflected (or displayed) in the final results?

Given that many of the model parameters are uncertain, it is essential to display the uncertainty. Otherwise, we are just not telling the truth. The approach that has worked well for us is described in Section 4 of PLG-0209 (see Reference 4). It is important for the decision-maker to have a full view of the analyst's state-of-knowledge--it instantly communicates the depth and thoroughness of the analysis. Point estimates are only a small piece of the information at best and at worst can mislead the decision-maker. Please see the enclosures.

8. What are your views on the "Limitation and Problem Areas" as discussed in the draft report?

It seems to me that this section is saying what is said in my response to Question 6. That is, we are only limited by the shortcomings of the integrated model of the plant under consideration. Thus, I am in agreement with the observations made. I do believe that the decision analysis problems noted ("dimensionality") are solvable. This is an area where less than vigorous approaches can be adopted at great savings in cost without compromising the analysis.

References

1. Lloyd, D. K., Lipou, M., "Reliability: Management, Methods, and Mathematics," Appendix 9A, "A Technique for Reliability Apportionment," Second Edition, 1979.

2. Garrick, B. J., et al., "Power Plant Availability Engineering," Appendix B, "Availability Targets and Allocations," EPRI NP-2168, May 1982.

3. General Dynamics, "Reliability and Maintainability Training Handbook," Chapter 6, "Apportionment," NAV SHIPS 9099-002-3000, 1964.

4. Kaplan, S., et al., "Methodology for Probabilistic Risk Assessment of Nuclear Power Plants," PLG-0209, June 1981.

F.3.3 Comments by Elias P. Gyftopoulos

I was pleased to see you again at the Steering Group Meeting for Guidelines and Criteria for Reliability Allocation in Bethesda on March 19, 1984.

I enjoyed reading the report by Cho and Papazoglou, dated January 1984, and listening to the presentations at the meeting. I have some minor comments.

1. Objectives 1 and 3 on page 1 of the report are well defined but objectives 2 and 4 are not. To allocate reliability to safety functions, plant systems, etc., we must use some a priori criteria, and develop a methodology to achieve results consistent with the criteria. If so, I see neither how the methodology will be used to develop allocation criteria, nor the meaning of the term "allocated criteria."

2. What is Task 2? Is the information mentioned in this task related to safety goals, allocation criteria, and allocation methodologies or to statistical information regarding reliabilities, costs and values of specific safety systems etc.?

3. The report recognizes the difficulty in establishing quantitative safety goals. Yet a major objective of the work is to establish criteria for a refined allocation of reliabilities consistent with these uncertain goals. Is the ambiguity about the values of the safety goals larger than the freedom we have in allocating reliabilities? I wonder whether the answer to this question should be part of your work. I am not positive about this suggestion because I am not clear about the ultimate use of the results of your program.

4. Some care should be exercised to distinguish between goals, criteria, and conditions so as to avoid confusion. For example, X early fatalities is a goal. $Y per fatality is a criterion, and X responses per demand for the AFWS is a condition. Is that your usage of these terms?

5. I agree that the definition of a reliability cost is fraught with uncertainty (page 5). However, the alternative of neglecting cost considerations from reactor safety discussions is disastrous not only for utilities but, most importantly, for rate payers (see, for example, Shoreham, Seabrook and many other unfinished power plants). For this reason, it is of paramount importance to include cost considerations in the program because above a certain level of either $/kw or $/kwh nuclear power becomes socially unacceptable.

It is true that indiscriminate use of cost functionals as optimality criteria may mask important trade-offs among safety goals. However, it is even

more true that indiscriminate neglect of cost considerations may result in safe but useless plants.

6. The assertion "that the lower the unavailability of the system the higher the cost or the degree of difficulty in achieving it" (page 7) is correct but not always. For example, a more reliable valve may be more expensive; however, the alternative of eliminating the valve may be costless. I believe that the possibility of design modifications (prior to freezing the design!) should be included in the discussion because it provides an additional important dimension to the problem.

7. I wonder whether the freedom of choice delegated to decision makers (page 8 and thereafter) is so broad that they would feel just as confused with the results of the analysis as without them. I believe that this concern is especially relevant to situations for which reliabilities can be varied discontinuously rather than continuously.

8. The basic properties of a reliability cost function of a component listed on page 14 are reasonable. However, comment 6 above should also be considered.

9. I agree with the limitations outlined on pp. 27 and 28. I wonder how you propose to treat dependent and common cause failures which may render some reliability allocations impossible.

10. I am not clear how the results of the program will be used. Knowledge of this usage is important because it may affect the choice of goals, criteria, and trade-offs.

11. My preference would be for analyses of specific plants rather than a generic approach. The reason is that a generic approach may give the erroneous impression that there is much more freedom in allocating reliabilities than there exists in specific power plants that are available in the market.

12. In general, I agree with Dr. Thadani that regardless of the outcome, the program will provide beneficial information.

Finally, I did not fully understand the comments by Professor Howard. If you receive a written report from him, I would appreciate receiving a copy because I have some views of my own on the frequency and ignorance interpretation of probabilities.

F.3.4 Comments by Ronald A. Howard

I am very pleased to see both from the report we read and from this meeting that the problems of nuclear regulation are being approached analytically and with openness of mind. In that spirit, I am happy to provide these comments on the contents on the report and on the general idea of probabilistic safety goals.

First, the idea of regulation by probability constraint has inherent logical flaws. As I demonstrated at the meeting, one of the principles of decision theory is that no piece of information can have a negative value in decision making. Yet, as I also showed by example, regulation by probability

constraint can cause a negative value of information and hence lead the person regulated to avoid testing or inspection in cases where it would otherwise be potentially valuable. As a result, it is never wise to have a probability constraint as part of a decision process.

Second, as far as specific comments on your report are concerned, I have two points I would like to emphasize. The first is the problem of dependence among your outcome measures. While the people working on the report are aware of this problem, I am not sure they appreciate the care necessary to handle this issue appropriately. There is an increase in dimensionality caused by dependence that can be overwhelming if not carefully handled.

Also, in connection with the present report, I question the wisdom of searching the outcome space with its huge dimensionality rather than the more modest decision space. The outcome space contains many points that are either physically or practically unreachable. I would concentrate on the decision space.

Third, I believe that your goal or establishing a rationale for achieving the proper design of subsystems would be best achieved by a process of decision system decomposition*. Once the overarching system is well defined, the proper boundary values for the subsystems can be derived. To do this, I would suggest assigning numerical values to the true outcome variables--core melt, acute fatalities, and latent fatalities. I have suggestions on numbers if you wish. Then you would solve the decomposition problem for the subsystems in the knowledge that their design decisions will be appropriately derived. Questions about the sensitivity of the results to the value numbers used can be investigated as a standard sensitivity analysis.

As I mentioned at the meeting, safety decisions are not just a matter of logic applied to agreed-upon information. They intimately require the assignment of values. To pretend that the question of safety regulation is a purely scientific problem is both logically wrong and the source of much of the mischief in the nuclear industry that we have seen. I am very pleased that we can begin to address this problem in the proper context.

*References

Dean W. Boyd, "Methodology for Analyzing Decision Problems Involving Complex Preference Assessments", dissertation, Engineering-Economic Systems Department, Stanford University, May 1970.

Edward G. Cazalet, "Decomposition of Complex Decision Problems with Applications to Electrical Power Systems Planning", dissertation, Engineering-Economic Systems Department, Stanford University, May 1970.

Larry D. Brandt, "Coordination of Decision Analyses within Decentralized Organizations", dissertation, Engineering-Economic Systems Department, Stanford University, March 1980.

F.3.5 Comments by F. Stan Nowlan

Question 3

In the United States the Federal Aviation Administration (FAA) is the regulatory body responsible for aviation safety. The process by which it controls safety of Transport Category aircraft includes:

(1) Airworthiness codes that define design requirements for such airplanes and their power plants.

(2) Issuance of Approved Type Certificates to manufacturers which certify that specific airplane designs comply with the requirements of the airworthiness code.

(3) Issuance of Production Certificates to manufacturers which certify that they are competent to manufacture aircraft and engines which will embody the characteristics of the approved design.

(4) Issuance of an Operations Specification to an air carrier which certifies (among other things) that the air carrier has the necessary training programs to ensure that the operating crews are familiar with the design capabilities of the airplane, and that the carrier has the maintenance capabilities (including its preventive maintenance program) to preserve the inherent design reliability and safety characteristics of the airplane.

Airworthiness codes are couched in terms that are most meaningful to designers. Nevertheless they have the end result of requiring that:

(1) Failure events (either loss of function or secondary damage associated with the failure mode involved) will not have a direct adverse effect on operating safety

or

Preventive maintenance has the capability of preventing the specific failure event that would adversely affect operating safety

or

Any loss of function that the operating crew cannot perform (that of the autoland system in bad weather) or combination of events that would adversely affect operating safety is extremely improbable. Extreme improbability is defined as not greater than 1 in 10^9 flights or flight hours, as applicable.

Failure tolerance with regard to loss of function is usually achieved by redundancy. Failure prevention sometimes depends upon use of safe-life limits of aircraft or engine parts subject to fatigue deterioration, but more often it depends upon diagnostic techniques that enable incipient failures to be discovered and corrected. Extreme probability, of course, depends upon a form of probabilistic risk assessment.

The airworthiness codes and regulatory processes of all major Western nations are very similar. However, it is not possible to enumerate the "calculated risk" associated with such codes. The codes become increasingly more

severe year by year as experience indicates the need to prevent recurrence of safety-related incidents. Frequently increased severity is retroactive.

Transport Category airplanes make about 10,000,000 flights a year. They also experience about 10,000,000 failure events a year. The fatal accident rate where mechanical failures are involved is of the order of 1 or 2 per 10,000,000 flights, and some of these involve personnel error or even intentional noncompliance with pertinent regulations. Some of them involve entirely unanticipated events such as sequences of failures which were not covered during probabilistic risk analysis, or extremely hostile meteorological conditions. Design characteristics cater to such things as complete loss of power by an engine, or deterioration of structure before it is discovered and repaired. However, there are rare cases under severe atmospheric conditions where aircraft run out of performance when loss of engine power is not involved; or structure which has not deteriorated breaks. These might be classified, perhaps, as risks due to external events. It appears that risk assessment is not a very precise science when dealing with extremely rare events.

Over and beyond the airworthiness requirements directed at disassociating failure events and safety, there are requirements directed at enhancing crash worthiness and survivability if an accident does occur. These are exemplified by such things as emergency evacuation capabilities, ditching capabilities, seat retention requirements, cabin material flammability requirements, individual oxygen masks and so on. To the best of my knowledge there never has been an attempt to relax these final safety requirements in light of the ever decreasing likelihood of requiring them in an accident caused by mechanical failures. In fact the crashworthiness and survivability requirements, as well as the basic design and operational ones, are becoming ever more stringent.

During the final stages of the Type Certification process the FAA, following proposals submitted by the designer and a group of operators, issues a Maintenance Review Board Document that details the minimum scheduled maintenance requirements necessary to protect the inherent design level of safety. Maintenance capabilities must be matched to design characteristics.

It is interesting to note that the Airworthiness Office at FAA Head quarters has cognizance over both design engineering and operator maintenance activities.

In the air transport community it has been possible to almost entirely divorce adverse safety consequences from reliability problems by an objective regulatory process. The volume of printed regulations is not large. The time period required to design a new airplane, test and certificate it, and deliver it to air carriers is of the order of four calendar years. Despite an extremely low exposure to accidents caused by mechanical failure events, other reasons for accidents do persist and crashworthiness and survival requirements are becoming increasingly stringent.

I don't think the basic objective of the Reliability Allocation study would be admissible in air transportation.

Question 1

I believe that the objectives of the Reliability Allocation program are well defined. However, with my own peculiar background I find the principle of a minimum cost tradeoff between the basic reliability characteristics of the operating plant and those of its safety systems hard to accept.

Question 2

The methodology seems rational once the basic objective is accepted. However, I believe that Professor Howard said that the methodology nullified the value of added information. That would be an undesirable feature.

Question 4

No comment.

Question 5

Cost models would seem to be the proper tool for evaluating tradeoffs, although they are difficult to define. Is it possible to estimate the order of magnitude of potential savings; i.e., 1 percent of total plant cost, 5 percent, 10 percent . . . .

Question 6

I assume that individual plants vary in their design characteristics, and hence in their exposure to hazardous failure events. If this is the case I would think that plant-specific PRA's would be necessary. In fact I am surprised that they are not required at present.

Question 7

No comment.

Question 8

The limitations and problem areas discussed in the report are real. However I am not at all clear how the reliability models cater to the interaction of maintenance and operating policies with design characteristics of the plant. In aviation at least, this interaction has to be recognized.

F.4 Discussions on Comments of the Steering Group Members*

We are grateful for the comments of the members of the Steering Group. Although we might not agree with all of them, they were invaluable in helping us focus the discussion and identify the existing difficulties both in the technical area and in the area of communicating the objectives and the methods of our study. In the first three sections of this status report, we tried to collectively respond to these comments of the Steering Group. In this section, we address the specific comments in greater detail.

*These discussions were provided in the second interim report dated May 1984.

F.4.1 Discussions on Comments by George W. Cunningham

We agree with the three general comments of Dr. Cunningham:

1. We continued with a specific example while at the same time we are actively pursuing alternate approaches or variations.

2. The question of the feasibility of a generic solution was discussed in Section 2.

3. We agree on the importance of the plant availability and on the need of examining it in connection with plant safety. There are two aspects of this issue. Theoretically, a certain level of safety can be achieved by different combinations of "prevention" and "mitigation" levels. The frequency of the accident initiators is directly related to "prevention". A well run plant will be characterized by low frequencies of plant transients or small LOCAs. On the other hand, a certain level of safety system reliability (mitigation) might be achieved at the expense of the plant availability. Inclusion of the initiators in the decision space with corresponding cost functions would provide a balance between prevention (low frequency for initiators) and mitigation (high reliability of safety systems). The present state-of-the-art does not provide, however, a good representation of the impact of a certain level of safety system reliability on plant availability. Recently, this impact has been considered in probabilistic studies for the determination of Limiting Conditions of Operation for safety systems in nuclear power plants. By an extension of our model, the impact of a particular reliability level on the plant availability could be expressed as additional cost. It should be noted that in the terminology of safety analysis, the "safety systems" that prevent core damage are characterized as "preventing" systems (preventing core damage) while the containment and associated safety systems are called mitigating (mitigating the results of core damage) systems. This aspect of prevention/mitigation is already included in the analysis. As a matter of fact the inclusion of the core damage frequency as an attribute emphasizes the special importance of prevention.

F.4.2 Discussions on Comments by B. John Garrick

We think we agree with most of Dr. Garrick's comments. Where we do not agree it may be a difference of semantics.

Dr. Garrick calls the reliability allocation idea infeasible. This statement in itself appears to be too general. Clearly, given a system reliability level, it can be allocated to component reliabilities in a large number of ways. The problem that we and Dr. Garrick share is how the system reliability level to be allocated has been determined, or equivalently, whether the reliability level is in itself a meaningful evaluator of the system. Cost considerations must be included. We tried to stress that point both in our first report and in the first Steering Group meeting and we repeat it here. What we mean by "reliability allocation" is the determination of sets of "component" reliabilities that imply attribute values that cannot be compared among themselves without a preference assessment. This preference assessment (which Dr. Garrick calls cost/risk/benefit tradeoff) is the natural next step which, however, we feel is outside the scope of our current study. Of course, we are eager to pursue this subject with the U.S. NRC. What we are trying to

do here is to provide a set of "component"* performance criteria (reliability indices) that are inherently consistent with the logic structure of a system and which result in a specific score in the set of attributes that characterize the performance of the system (for the purposes of this study these attributes are: frequency of core damage, expected acute and latent fatalities and cost). In that sense we do not think that we are trying to answer the question of "how safe is safe enough?" but a more reasonable one that includes cost/risk/benefit considerations.

Another point that Dr. Garrick helped us clarify is the nature of the proposed approach. As we tried to explain in Section 3 of this note, we do not consider the proposed approach as "backward". We too start from the set of "feasible" λ_i (x_i in our terminology), we find their effect on the performance indices (attributes), and we reject the ones that are obviously non-optimal (inferior). In doing so, we have a somewhat richer field of x_i(**) than what Dr. Garrick claims exists in reality (see p. 7 of this report). Recognizing the fact that our study does not cover only existing plants this is a desired characteristic. Up to this point we think the proposed approach is as "forward" or "decision theoretic" as any other approach.

Having settled on the semantics, we agree with what we think are Dr. Garrick's main points.

- More than one attribute is necessary (including cost).
- Eventually a preference assessment (among the attributes) is necessary.
- There are problems with the dependences and the existence of a generic solution.

F.4.3 Discussions on Comments by Elias P. Gyftopoulos

We tried to respond to comments #1, #3, #7 and #10 in Sections 2 and 3 of the present writeup. As a matter of fact questions #3 and #10 were the major motivation for Section 2.

Some effort has been made to use the terms goals, criteria, and conditions consistently. We hope that future versions of the report will be even more consistent in the usage of these terms. We use the terms Objectives, Attributes and Goals as they are defined by Keeney and Raiffa in Ref. 13.

> "An objective generally indicate the "direction" in which we should strive to do better". For example, decrease likelihood of core damage, decrease cost.
>
> "An attribute measures quantitatively the degree of achievement or satisfaction of a specific objective". For example, 10^{-4}/year frequency of core damage, $\$2 \times 10^{9}$ for cost.

*These discussions were provided in the second interim report dated May 1984.
**Our x_i do not necessarily cover the whole theoretical range of values [i.e., (0,1)]. They are rather defined to cover whatever values are realistically achievable. Some of them can take only one value.

"A goal identifies a specific level of achievement to strive toward". A goal can either be achieved or not. The frequency of core damage must be less than 10^{-3}/year and the cost less than $\$2 \times 10^{9}$ are goals.

The term criterion is loosely used interchangeably with the term goal.

6.-8. Situations like the one mentioned in this comment ought to be reflected in the cost function. The discontinuities introduced in the cost functions, however, complicate the computational aspects of the problem.

9. We intend to include dependences in the logic model for the plant the same way they are incorporated in state-of-the-art PRAs.

11. We are trying to address this point in the example. We are using a specific plant as a model and we would like to compare the results with the characteristics of the plant itself as well as with those of other similar plants.

F.4.4 Discussions on Comments by Ronald A. Howard

Professor Howard, at the first meeting of the Steering Group and in his followup written comments, made a very important comment about "regulation by probability constraints" and demonstrated by a simple example the potential logical flaws of such an approach. We fully agree with the underlying principles of Prof. Howard's comment. We would like, however, to clarify the issue lest the wrong impression will be created that probability constraints are inherently impossible or that they necessarily lead to logical inconsistencies.

1. The position of the BNL team is that decisions about nuclear safety should be based both on information about system behavior and on the relative values of the various desired and undesired possible consequences. Given this basic premise, we believe that probability constraints can be derived from a given set of assigned values on the possible outcomes of interest. The important point is that the probability constraints should be derived from the assessed relative values of the outcomes or at least that the decision makers should be aware of the value assessments implied by the probability constraints. Inconsistencies arising from probability constraints are then simply inconsistencies due to different value assessments by different persons or different groups of persons.

   The example that Prof. Howard presented in the first meeting demonstrates these points. We will repeat here only the parts that are necessary for our discussion. The example considered a simple two alternative problem; a patient must decide on whether to undergo an operation (alternative α_1) or not (alternative α_2). The corresponding decision tree is depicted in Figure 2.

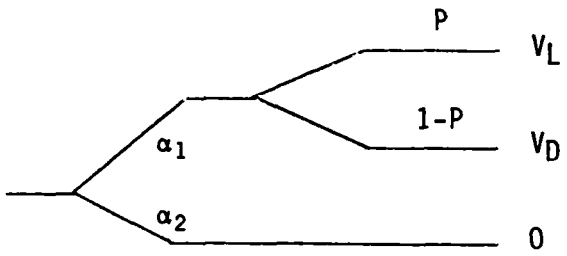


Figure 2

If the patient chooses the operation he will live with probability p, or die with probability 1-p. A value is assigned by the patient to each outcome (V_L for successful operation, V_D for an unsuccessful operation). For the sake of simplicity no life or death outcomes were examined for alternative (α_2) and a reference value of zero was as signed to this alternative. According to the principles of decision analysis the decision maker (patient) will choose the alternative that is characterized by the maximum expected value. (We assume here that the values assigned include uncertainty considerations and that they are in fact utilities). Denoting expectation by E we then get for the expected values of the two alternatives

$$E\,[V(\alpha_1)] = pV_L + (1-p)V_D \qquad (1)$$

$$E\,[V(\alpha_2)] = 0 \qquad (2)$$

The patient will choose alternative α_1 over α_2 only if

$$E\,[V(\alpha_1)] > E\,[V(\alpha_2)] \quad \text{or if}$$

$$pV_L + (1-p)V_D > 0 \quad \text{or if}$$

$$p > -\frac{V_D}{V_L - V_D} \qquad (3)$$

In the example, Prof. Howard used the values of $V_D = -2\times10^6$ and $V_L=1\times10^6$ ($) so that Eq. (3) implies that

$$p > \frac{2}{3} \quad \text{or} \quad p > 0.6666 \qquad (4)$$

In other words, the patient has implicitly defined a probability constraint: He will undergo the operation if the probability of success is higher than 2/3. This constraint depends on the relative values he assigns to life or death after the operation and to the option of not undergoing the operation. It is a probability constraint, however, and it can be used in deciding on whether to have the operation or not.

Later in the example, a hospital rule is invoked according to which an operation is performed by the hospital only if the probability of success is higher than 4/5 (or 0.80). By virtue of with Eq. (3) this different probability constraint implies different values for the possible outcomes of our decision problem. The value of life and death is different for the hospital than for the individual patient. Given these different values it is not surprising that the example leads to logical inconsistencies. It is important, however, to emphasize that it is this difference (inconsistency) in the assigned values that generated the problem and not the use of probability constraints per se. The hospital might have reached its rule of "operate if p > 0.80" through an entirely logical and sound thought process and evaluation. What is of concern to the patient, however, is that the implied values on the outcomes of interest are different than his own values. That's where the effort for resolving the conflict should be concentrated.

The purpose of this discussion is not to argue that probabilistic constraints are always possible to be defined and meaningful but that they do not necessarily lead to logical inconsistencies. The question of the value assessment for a core melt event is a very important one. As was discussed in the meeting, an accident in a nuclear power plant that involves core damage has implications that go beyond the specific health and economic consequences of the accident. Even if the health effects are negligible, such an accident will probably have a significant impact on the whole nuclear industry. The impact of a core melt, therefore, can not necessarily be measured in terms of other attributes or evaluation indices of the nuclear power plants (i.e., health and economic effects). It rather has a value of its own. It must, therefore, be included as an attribute in the evaluation of a nuclear power plant. Once this has been agreed upon, and a value has been assigned, then under certain circumstances the assigned value can be translated into a probability constraint. The conditions and circumstances under

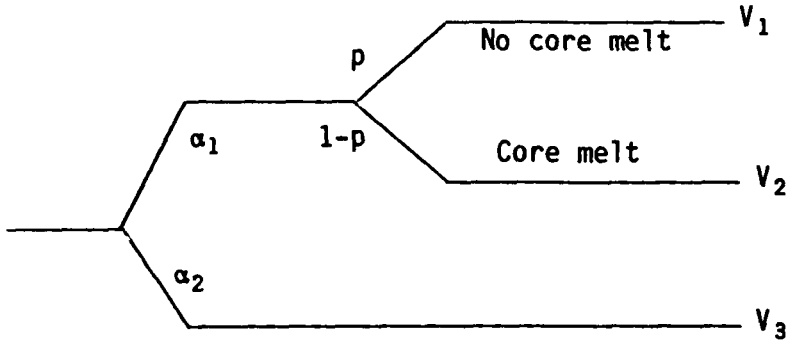


Figure 3

which this can be done, however, need very careful consideration. Here, again, the problem of different value assessments by different decision makers is very important and could lead to logical inconsistencies. To highlight the problem of different value assessments let us consider a hypothetical example of how a constraint on the

frequency of core damage could be established by two different decision makers. The first decision maker is the Nuclear Regulatory Commission which decides on nuclear matters on behalf of the nation and it is faced with a choice between the following two alternatives:

α_1 Follow the nuclear option and go ahead with the construction and operation of 200 nuclear power plants, each to operate for 30 years.

α_2 Forego the nuclear option and satisfy the corresponding energy needs with other means.

If alternative α_1 is chosen, then a core melt in any of the nuclear plants might or might not happen. The corresponding decision tree is shown in Figure 3. Because of the adverse public reaction it is assumed that the first core-melt down will cause the shutdown of all operating nuclear power plants. The probability of no core damage in any of the nuclear plants during the T years of the plant life is given by

$$p = e^{-\lambda NT} \tag{5}$$

where it was assumed that a core damage occurs according to a poisson random process with intensity λ. Assigning values V_1, V_2 and V_3 to the three possible outcomes in the tree and applying the maximum expected value (utility) principle we find the alternative α_1 would be chosen if

$$e^{-\lambda NT} > \frac{V_3 - V_2}{V_1 - V_2} \tag{6}$$

which implies a "probability constraint" on λ

$$\lambda < \frac{-\ln \dfrac{V_3 - V_2}{V_1 - V_2}}{NT} \ . \tag{7}$$

For example, if $V_1-V_2 = 2(V_3-V_2)$, N = 200, and T = 30y, Eq. (7) implies that

$$\lambda < 1.15 \times 10^{-4}\ y^{-1} \ . \tag{8}$$

Different value assessment (always on a national basis) would result in different constraints.

A utility company, on the other hand, facing the question of whether to build one nuclear plant could describe its decision problem with a similar decision tree (as in Figure 3) where now the probability of no core damage is $P=e^{-\lambda T}$ and V_1', V_2', V_3' are the values assigned to the three outcomes by the utility decision makers. The resulting constraint on the frequency λ is

$$\lambda < \frac{-\ln \frac{V_3 - V_2}{V_1 - V_2}}{T} \qquad (9)$$

which will in general be different from (8).

In conclusion, the BNL team recognizes the importance of the probability constraints and the implied value assessments. We believe that "reduce likelihood of core damage" should be retained as an objective. We acknowledge the fact that value assessment is necessary for a consistent and rational regulatory decision making process. We also acknowledge the fact that a value assessment does not necessarily imply a well defined probability constraint. We consider, however, this problem as part of the general preference assessment problem mentioned in Section 3.1 and as such out of the scope of this study. We propose to keep the frequency of core damage as an attribute for the safety evaluation of nuclear power plants while at the same time we will emphasize the implications and the conditions under which such a treatment is valid.

2. Prof. Howard is also concerned about the questions of dependences and their proper handling. The handling of dependences for the purposes of this study is described elsewhere in this report. In general, we tried to follow the present state-of-the-art in nuclear PRAs. We welcome, however, specific recommendations that Prof. Howard might have in mind.

3. The third comment by Prof. Howard addresses the problem of the dimensionality of the outcome space. A similar comment was made by Dr. Garrick and we addressed it in our response to Dr. Garrick's comments.

4. Finally, Prof. Howard suggests the use of a decomposition approach presented in a series of three dissertations. We are actively examining the applicability of this approach to our problem. A preliminary review of the proposed methodology indicates that it will be applicable under conditions of preferential and utility independence.

   It should be noted, however, that again we enter the general area of preference assessment which is not part of our mandate.

F.4.5 Discussions on Comments by F. Stan Nowlan

Mr. Nowlan introduced to us an example that safety goals are currently in place, that is, the aviation industry. He also showed a concern on the idea of tradeoffs among the safety goals or performance criteria. We tried to convey in our first report and in the main body of the present report the necessity as well as the difficulty of making value tradeoffs.

The other point which Mr. Nowlan was curious about was how the reliability models in PRAs treat the interaction of maintenance and operating policies with design characteristics of the plant. The current state-of-the-art PRAs

include maintenance and operational aspects in the safety evaluation. Their effects are usually manifested in unavailabilities (x_i's in our notation) of the components or in additional x_i's.

REFERENCES FOR TECHNICAL APPENDICES

1. Okrent, D., Apostolakis, G., Whitley, R., Garrick, B. J., "On PRA Quality and Use", Chapter 4, UCLA-ENG-8269, October 1982.

2. U.S. Nuclear Regulatory Commission, "Safety Goals for Nuclear Power Plant Operation", NUREG-0880, Revision 1, May 1983.

3. Fischhoff, B., "Standard Setting Standards: A Systematic Approach to Managing Public Health and Safety Risks", Decision Research, NUREG/CR-3508, February 1984.

4. Papazoglou, I. A., et al., "A Review of the Limerick Generating Station Probabilistic Risk Assessment", Brookhaven National Laboratory, NUREG/CR-3028, February 1983.

5. Philadelphia Electric Company, "Probabilistic Risk Assessment Limerick Generating Station", Docket Nos. 50-352, 353, June 1982.

6. Joksimovich, V., et al., "A Review of Some Early Large Scale PRA Studies", NUS Corporation, EPRI NP-3265, October 1983.

7. U.S. Nuclear Regulatory Commission, "Probabilistic Risk Assessment (PRA) Reference Document", NUREG-1050, September 1984.

8. Kaplan, S., "Matrix Theory Formalism for Event Tree Analysis: Application to Nuclear-Risk Analysis", Risk Analysis, 2, 9, 1982.

9. Aggarwal, K. K., Gupta, J. S., "On Minimizing the Cost of Reliable Systems", IEEE Trans. Rel. R-24, 205, 1975.

10. Garrick, B. J., "Examining the Realities of Risk Management", Presented at the Society for Risk Analysis 1984 Annual Meeting, Knoxville, TN, September 30 - October 3, 1984.

11. Cohon, J. L., Multiobjective Programming and Planning, Academic Press, New York, 1978.

12. Goicoechea, A., Hansen, D. R., Duckstein, L., Multiobjective Decision Analysis with Engineering and Business Applications, John Wiley and Sons, New York, 1982.

13. Keeney, R., Raiffa, H., Decisions with Multiple Objectives: Preferences and Value Tradeoffs, Wiley, New York, 1976.

14. Numerical Algorithms Group, Fortran Library Manual Mark 10, 1983.

15. Luenberger, D. G., Introduction to Linear and Nonlinear Programming, Addison-Wesley, Reading, MA, 1973.

16. Fleming, K. N., "A Reliability Model for Common Mode Failures in Redundant Safety Systems", Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation, April 24, 1975.

17. Apostolaksis, G. and Kaplan, S., "Pitfalls in Risk Calculations", Reliability Engineering, 2, 135, 1981.

18. Kennedy, R. P., et al., "Probabilistic Seismic Safety Study of an Existing Nuclear Power Plant", Nuclear Engineering and Design, 59, 315, 1980.

19. Azarm, M. A., et al., "A Review of the Limerick Generating Station Severe Accident Risk Assessment", Brookhaven National Laboratory, NUREG/CR-3493, January 1984.

20. Philadelphia Electric Company, "Severe Accident Risk Assessment Limerick Generating Station", Report No. 4161, April 1983.

21. Howard, R. A., "The Foundations of Decision Analysis", IEEE Trans. Syst. Sci. Cybernet. SSC-4, 211, 1968.

22. Boyd, D. W., "A Methodology for Analyzing Decision Problems Involving Complex Preference Assessments", Ph.D. Dissertation, Stanford University, May 1970.

23. American Nuclear Society, Institute for Electrical and Electronics Engineers, "A PRA Procedures Guide", NUREG/CR-2300, January 1983.

24. Nemhauser, G. and Garfinkel, R., Integer Programming, John Wiley, New York, 1972.

25. Barlow, R. E. and Proschan, F., Mathematical Theory of Reliability, John Wiley & Sons, New York, 1965.

C FORM 335 (4) CM 1102, 1, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

INSTRUCTIONS ON THE REVERSE

1 REPORT NUMBER (Assigned by TIDC, add Vol No., if any)
NUREG/CR-4048
BNL-NUREG-51834

TITLE AND SUBTITLE
A Methodology for Allocating Reliability and Risk

3 LEAVE BLANK

4 DATE REPORT COMPLETED
MONTH: March YEAR: 1986

AUTHOR(S)
N. Z. Cho, I. A. Papazoglou, R. A. Bari

6 DATE REPORT ISSUED
MONTH: May YEAR: 1986

PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Brookhaven National Laboratory
Upton, New York 11973

8 PROJECT/TASK/WORK UNIT NUMBER

9 FIN OR GRANT NUMBER
FIN A-3728

SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Safety Review and Oversight
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555

11a. TYPE OF REPORT

b. PERIOD COVERED (Inclusive dates)

SUPPLEMENTARY NOTES

ABSTRACT (200 words or less)

This report describes a methodology for reliability and risk allocation in nuclear power plants. The work investigates the technical feasibility of allocating reliability and risk expressed in a set of global safety criteria to various reactor systems, subsystems, components, operations, and structures in a consistent manner.

The problem is formulated as a multiattribute decision analysis paradigm. The work mainly addresses the first two steps of a typical decision analysis, i.e., (1) identifying alternatives and (2) generating information on outcomes of the alternatives, by performing a multiobjective optimization on a PRA model and reliability cost functions. The multiobjective optimization serves as the guiding principle to reliability and risk allocation.

The concept of "noninferiority" is used in the multiobjective optimization problem. Finding the noninferior solution set is the main theme of the current approach. The final step of decision analysis, i.e., assessment of the decision maker's preferences could then be performed more easily on the noninferior solution set.

Results of the methodology applications to a nontrivial risk model are provided, and several outstanding issues such as generic allocation, preference assessment, and uncertainty are discussed.

DOCUMENT ANALYSIS - a KEYWORDS/DESCRIPTORS

Reliability Allocation
Multiobjective Optimization
Noninferior Solutions
Safety Goals for Nuclear Power Plants
Probabilistic Risk Assessments

IDENTIFIERS/OPEN-ENDED TERMS

15. AVAILABILITY STATEMENT
Unlimited

16. SECURITY CLASSIFICATION
(This page) Unclassified
(This report) Unclassified

17. NUMBER OF PAGES

18 PRICE

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555