2

BNL-NUREG--35758

TI85 007484

A DECISION-THEORETIC METHODOLOGY FOR RELIABILITY AND RISK ALLOCATION IN NUCLEAR POWER PLANTS

N. Z. Cho, I. A. Papazoglou, and R. A. Bari
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, New York 11973

A. El-Bassioni
U.S. Nuclear Regulatory Commission

ABSTRACT

This paper decribes a methodology for allocating reliability and risk to various reactor systems, subsystems, components, operations, and structures in a consistent manner, based on a set of global safety criteria which are not rigid. The problem is formulated as a multiattribute decision analysis paradigm; the multiobjective optimization, which is performed on a PRA model and reliability cost functions, serves as the guiding principle for 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 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 and preference assessment are discussed.

I. INTRODUCTION

The purpose of this paper is to describe a decision-theoretic methodology for reliability and risk allocation in commercial nuclear power plants. The work was performed in support of the U. S. Nuclear Regulatory Commission Office of Nuclear Reactor Regulation's effort to investigate the technical feasibility of allocating reliability and risk to reactor systems, subsystems, components, structures, and operations such that the allocated reliabilities and risks are consistent with top

---

*This work was performed under the auspices of the U.S. Nuclear Regulatory Commission.
The views and opinions expressed herein are not necessarily those of the U.S. NRC.

level (or global) criteria for plant performance and public health risks. While NRC's proposed safety goals and numerical guidelines (1) provide an example of such top level criteria, the present work does not rely on those goals as a basis for its analysis.

The problem was formulated in the context of multiobjective (multiattribute) decision analysis. Decision analysis, which is a discipline concerned with helping individuals make decisions in complex decision problems, is decomposed usually into three steps (2,3): (1) Identifying choices or alternatives, (2) Generating information on outcomes (consequences) of the identified alternatives, and (3) Assessing the decision maker's preferences on the outcomes.

This paper focuses on the first two steps above, which were accomplished by the multiobjective optimization technique (4) with a PRA model and reliability cost information. A more detailed account of the work is given in Ref. 5.

II. METHODOLOGY

Before presenting the reliability/risk allocation methodology, we provide briefly the basic elements of the allocation framework: (1) A plant PRA model, (2) Reliability cost functions, and (3) Top level numerical safety criteria.

II.A Allocation Framework

1. PRA Models. Since the current PRA models provide the most comprehensive description of the relationships between the undesirable consequences (objective functions) and performance of major components, structures, and operations in nuclear power plants, a plant PRA model is the best available basis for risk related decision making.

A PRA model can be represented concisely in matrix formalism (6,7) as follows:

Core damage frequency $$C_d = \underline{f}\ \underline{M}\ \underline{u} \tag{1}$$

Expected acute fatalities $$A = \underline{f}\ \underline{M}\ \underline{C}\ \underline{s}(a) \tag{2}$$

Expected latent fatalities $$L = \underline{f}\ \underline{M}\ \underline{C}\ \underline{s}(\ell) \tag{3}$$

where $\underline{f}$ is the accident initiator (internal and external) frequency vector, $\underline{M}$ the plant damage matrix, $\underline{C}$ the containment matrix, $\underline{s}(a)$ and $\underline{s}(\ell)$ the site vectors for acute and latent fatalities respectively, and u is the column vector with elements equal to unity.

2. Reliability Cost Functions. A particular level of system or component reliability is achieved through the expenditure of resources and in addition there may be technological limits on the achievable levels of reliability. Thus, the lower the tolerable level of undesirable consequences, the higher the required reliability levels and the higher the needed resources or "cost." The "cost" implied by a particular reliability level is, therefore, a necessary element in any allocation problem. Reliability cost functions should represent the cost or the degree of difficulty in achieving specific levels of reliability. The required properties and various forms of cost functions are reported in the reliability literature and summarized in Ref. 5.

An expression for the total cost, in terms of individual component reliability cost functions, is

$$G = \sum_{i=1}^{n} g_i(x_i) \tag{4}$$

where x_i is the unreliability or unavailability of component i.

3. Top Level Numerical Safety Criteria. In general, it could perhaps be assumed that a set of numerical safety criteria is given on a global basis, e.g., C_d^*, A^*, and L^* for core damage frequency, expected acute fatalities, and expected latent fatalities, respectively. However, in the multiobjective optimization approach to be described below, the numerical safety criteria are themselves regarded as variables and are not treated as fixed constraints. This approach will give useful insights in arriving at more meaningful and consistent numerical safety criteria than an approach which begins with rigid criteria.

II.B Reliability/Risk Allocation

In the multiobjective optimization formulation, the objective functions and decision variables are the following:

Objective functions: $\underline{Z}$

1. Core damage frequency, C_d in Eq. (1)
2. Expected acute fatalities, A in Eq. (2)
3. Expected latent fatalities, L in Eq. (3)
4. Reliability cost, G in Eq. (4)

Decision variables: $\underline{X}$

1. Unavailabilities of safety systems and components, including human errors (affect the elements of $\underline{M}$)
2. Initiator frequencies (vector $\underline{f}$)
3. Containment failure probabilities (affect the elements of $\underline{C}$)

It is noted that the objective functions above may conflict with each other, i.e., a particular change in the decision variables may cause conflicting changes in the objective functions.

Formally, we want to:

$$\text{Minimize } \underline{Z}(\underline{X}) = [C_d(\underline{X}), A(\underline{X}), L(\underline{X}), G(\underline{X})] \tag{5}$$

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

where $\underline{Z}(\underline{X})$ is a four-dimensional vector composed of the objective functions and F_d the feasible region in decision space.

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. The concept called "noninferiority" (or "nondominance") is needed (4).

A solution $\underline{X}$ (and the corresponding $\underline{Z}(\underline{X})$ is called noninferior if there exists no feasible $\underline{X}'$ such that

$$\begin{aligned} C_d(\underline{X}') &\leq C_d(\underline{X}) \\ A(\underline{X}') &\leq A(\underline{X}) \\ L(\underline{X}') &\leq L(\underline{X}) \\ G(\underline{X}') &\leq G(\underline{X}) \end{aligned} \tag{6}$$

where the strict inequality holds for at least one objective. If such a feasible $\underline{X}'$ exists, then $\underline{X}$ (and the corresponding $\underline{Z}(\underline{X})$) is inferior.

The definition of the "noninferior set" is graphically depicted in Figure 1 for a two-dimensional case.

A technique to generate noninferior solutions and discard inferior solutions is the constraint method, i.e.,

$$\text{Minimize } z(\underline{X}) = G(\underline{X}) \tag{7}$$

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

$$C_d(\underline{X}) \leq \varepsilon_1$$

$$A(\underline{X}) \leq \varepsilon_2$$

$$L(\underline{X}) \leq \varepsilon_3.$$

The choice of $G(\underline{X})$ as the $z(\underline{X})$ is arbitrary. Any one of the four objective functions can serve as the $z(\underline{X})$. The ε's are varied parametrically to trace out noninferior solutions. A computer program was developed in Ref. 5 for this purpose.

Identification of the noninferior solutions by the multiobjective optimization approach as described above constitutes the first two steps of the decision analysis outlined in Section I. Comparison between any two solutions in the noninferior set and choosing one from the noninferior set involve value trade-offs (preference assessments) among the objective functions. This will be the third step in the decision analysis. The elements of a particular noninferior solution vector $\underline{X}$ singled out from the noninferior set by preference assessments are the allocated reliabilities and represent the "aspiration" levels toward which a plant would be designed or modified.

The preference assessment in the outcome space is a rather involved task, both because of the multitude of the attributes (objective functions) 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 that is understood about the decision problem, the easier it will be to articulate and understand the preferences on the outcomes. Therefore, the presentation of all noninferior solutions would facilitate the process of assessing and communicating the corresponding preferences. Thus, the current approach may be considered a decomposition approach in a spirit to that of Ref. 8.

III. RESULTS AND DISCUSSIONS

The allocation methodology was applied to a boiling water reactor with an existing PRA. The risk model (7) was modified and simplified* for the purpose of calculational convenience in order to illustrate the basic features of the methodology. It consists of 3 initiators, 15 accident sequences, and 19 decision variables. The three initiators are the most dominant contributors to core damage and health consequences, viz, (1) Loss of feedwater/main steam isolation valve closure, (2) Loss of offsite power, and (3) Turbine trip. (Ref. 5 further extends this base model to include a seismic sequence and to include containment performance parameters in the decision variables.) The accident sequences are combinations of failures and successes of "supercomponents" whose unavailabilities are the decision variables, e.g., reactor scram systems, high and low pressure coolant injection systems, residual heat removal system, feedwater and service water systems, diesel generator system, and several operator actions.

Figures 2 and 3 show the noninferior outcomes in two-dimensional displays. The noninferior outcomes are grouped in several core damage frequencies. For example, at 1×10^{-4} core damage probability per reactor year, the expected acute fatalities vary from 8.3×10^{-5} to 5.9×10^{-4}, the expected latent fatalities from 1.8×10^{-1} to 2.5×10^{-1} and the reliability costs from 5.6×10^{5} to 3.5×10^{5}.

We note from examining the two extreme points in each group (e.g., C1 and C8 in Figures 2 and 3) that the acute fatalities are rather low (e.g., compared to the various proposed safety goals) and that the latent fatalities is not a strong function of the cost. Based on this type of "informal" preference assessment, we may wish to retain only the noninferior solutions that imply the lowest cost from each group. These solutions (A6, B5, C8, D8) are tabulated in Table 1 along with the corresponding unavailabilities. Table 1 suggests very well defined performance criteria, for example, for the feedwater/power conversion systems [X(6)] and its recovery for containment heat removal purposes [X(19)]. However, systems such as the reactor protection system [X(1)], the DC power system [X(4)], and the residual heat removal system [X(14)] are not characterized by well defined performance criteria. Determination of more well defined criteria for these systems calls for an involved preference assessment.

---

*Thus no inferences should be drawn with regard to the safety or operation of the plant from which the present model was abstracted.

IV. CONCLUSIONS

The experience with applications of the allocation methodology described above demonstrates that allocation of reliability is technically feasible and that the methodology is operational. The methodology provides valuable information to the decision maker in that it offers the viable noninferior options (and only the viable noninferior options) for the set of top level criteria and their self-consistently associated lower level performance requirements and thus renders the viable options more amenable to a 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.

The design differences in the various nuclear power plants render a generic allocation difficult. For operating plants the methods developed here might be most useful in conjunction with operational practices, cost-effective retrofits, and exemptions from existing requirements. For future plants the methods would be a useful adjunct to the design of a safe and economical plant.

While information on the cost functions was identified as a necessary ingredient in the allocation scheme, the detailed and realistic specification of cost functions appears to be a difficult but not insurmountable 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 most situations the process of the methodology will serve as useful guidance to reliability design and improvement of nuclear reactor systems, which could be used to supplement more traditional methods. Thus, the methodology described in the paper can be used by plant designers, plant owners, or regulators as appropriate.

ACKNOWLEDGMENTS

We benefited from comments, discussions, and suggestions from many of our colleagues at Brookhaven National Laboratory and at the U. S. Nuclear Regulatory Commission and from members of a Steering Group that was formed for this project.

REFERENCES

1. U.S. Nuclear Regulatory Commission. "Safety Goals for Nuclear Power Plant Operation." NUREG-0880, Revision 1, May 1980.

2. R. A. Howard. "An Assessment of Decision Analysis." Operations Research, 28, 4, 1980.

3. R. L. Keeney and H. Raiffa. "Decisions with Multiple Objectives: Preferences and Value Tradeoffs." New York: John Wiley and Sons, 1976.

4. J. L. Cohon. "Multiobjective Programming and Planning." New York: Academic Press, 1978.

5. N. Z. Cho, I. A. Papazoglou, and R. A. Bari. "A Methodology for Allocating Reliability and Risk." Brookhaven National Laboratory, Draft NUREG/CR-4048, BNL-NUREG-51834, November 1984.

6. S. Kaplan et al. "Methodology for Probabilistic Risk Assessment of Nuclear Power Plants." Pickard, Lowe, and Garrick, Inc., PLG-0209, June 1981.

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

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

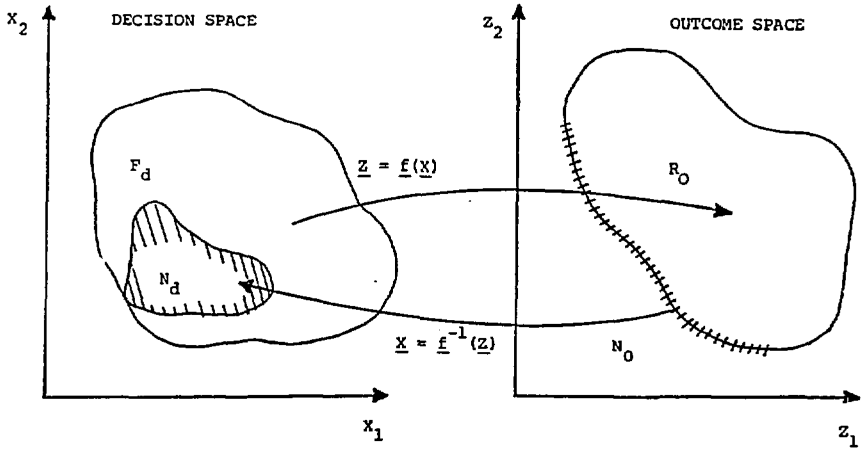

Figure 1. Mapping of Decision Space into Outcome Space

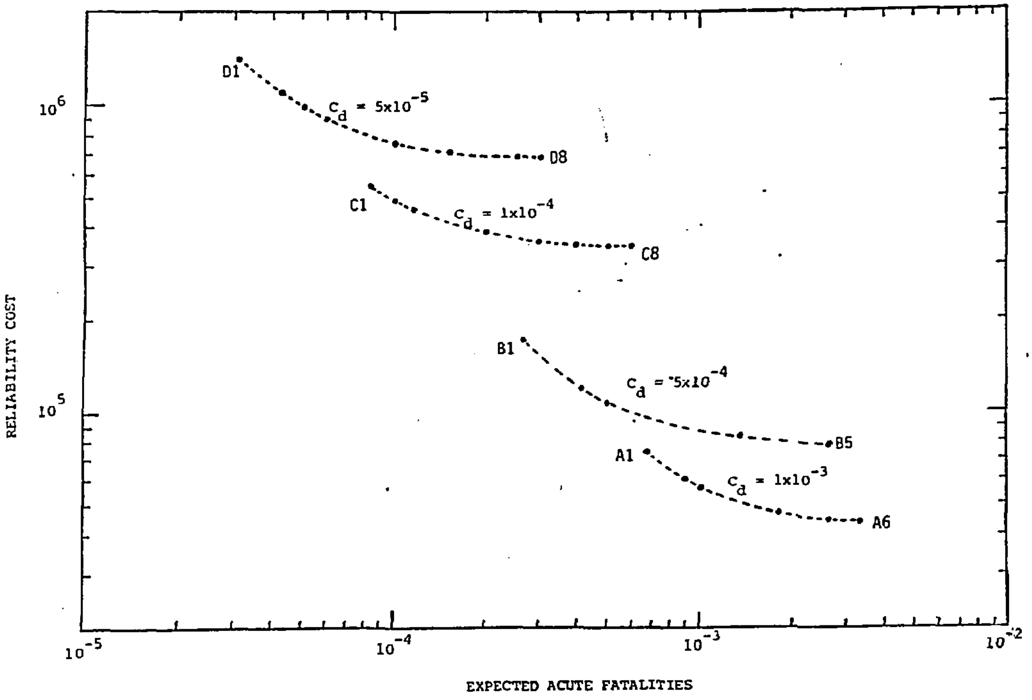

Figure 2. A Two-Dimensional Display of Noninferior Outcomes at Several Core Damage Frequencies

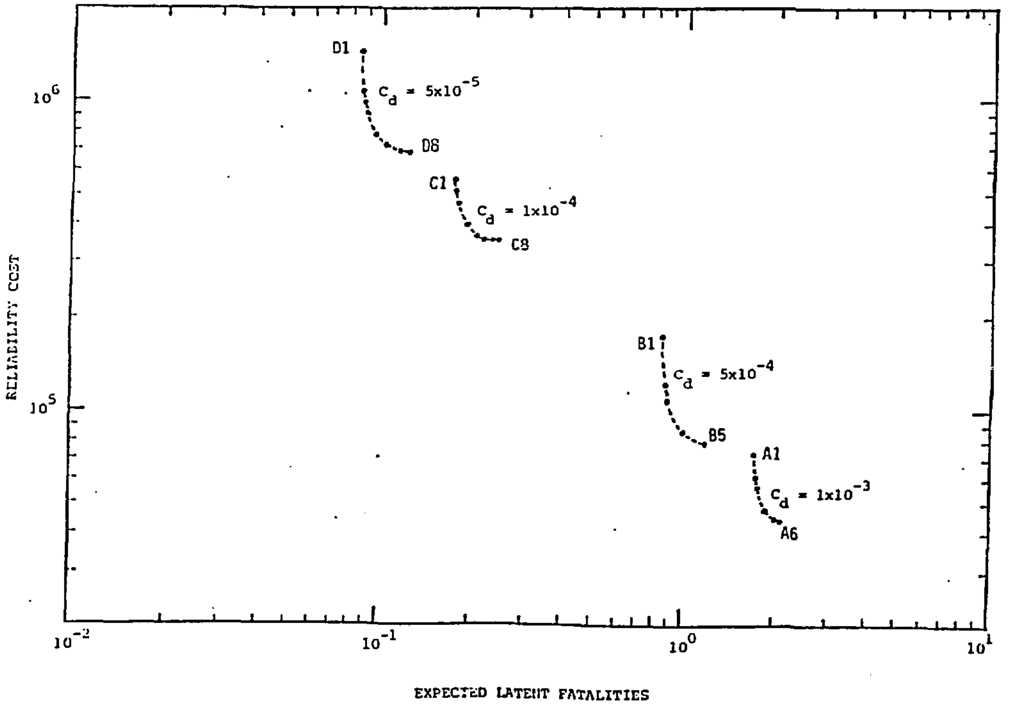

Figure 3. A Two-Dimensional Display of Noninferior Outcomes at Several Core Damage Frequencies

Table 1

NONINFERIOR SOLUTIONS WITH LEAST COST FROM EACH GROUP

		A6	B5	C8	D8
C_d		1.00(-3)	5.00(-4)	1.00(-4)	5.00(-5)
A		3.28(-3)	2.66(-3)	5.87(-4)	3.01(-4)
L		2.09(0)	1.19(0)	2.47(-1)	1.24(-1)
G		4.44(+4)	7.95(+4)	3.52(+5)	6.87(+5)
X(1)	RPS(M)	1.97(-3)	1.65(-3)	3.66(-4)	1.88(-4)
X(2)	SLCSH	1.34(-3)	7.27(-4)	3.15(-4)	2.21(-4)
X(3)	OSP	5.20(-4)	5.20(-4)	5.20(-4)	5.20(-4)
X(4)	EDC	5.49(-5)	2.73(-5)	5.57(-6)	2.80(-6)
X(5)	WSW	1.23(-4)	6.10(-5)	1.25(-5)	6.26(-6)
X(6)	FWPCS	8.42(-3)	5.31(-3)	5.00(-3)	5.00(-3)
X(7)	ARC	1.50(-1)	1.50(-1)	1.50(-1)	1.50(-1)
X(8)	RCICH	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(9)	HPCIH	1.00(-2)	1.00(-2)	1.00(-2)	1.00(-2)
X(10)	ADSH	1.40(-2)	6.79(-3)	1.43(-3)	7.20(-4)
X(11)	LPCIH	5.86(-2)	3.75(-2)	1.31(-2)	7.99(-3)
X(12)	LPCSH	5.70(-2)	3.56(-2)	1.23(-2)	8.09(-3)
X(13)	RECOV	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)
X(14)	RHRH	3.28(-3)	2.05(-3)	5.40(-4)	2.89(-4)
X(15)	FWPCSL	5.58(-3)	3.52(-3)	1.40(-3)	1.00(-3)
X(16)	DG	3.32(-3)	1.65(-3)	3.36(-4)	1.69(-4)
X(17)	X	1.40(-2)	7.44(-3)	1.43(-3)	7.20(-4)
X(18)	D	2.00(-3)	2.00(-3)	2.00(-3)	2.00(-3)
X(19)	FWPCSL(RECOV)	5.00(-2)	5.00(-2)	5.00(-2)	5.00(-2)