PROBABILISTIC RELATIONSHIPS IN
ACCEPTABLE RISK STUDIES

J. R. BENJAMIN
Engineering Decision Analysis Company, Inc. (EDAC)
480 California Avenue, Suite 301, Palo Alto, California 94306, U.S.A.

SUMMARY

Acceptable risk studies involve uncertainties in future events: consequences and associated values, the acceptability levels, and the future decision environment. Probabilistic procedures afford the basic analytical tool to study the influence of each of these parameters on the acceptable risk decision, including their interrelationships, and combinations. A series of examples are presented in the paper in increasing complexity to illustrate the principles involved and to quantify the relationships to the acceptable risk decision.

The basic objective of such studies is to broaden the scientific basis of acceptable risk decision making. It is shown that rationality and consistency in decision making is facilitated by such studies and that rather simple relationships exist in many situations of interest. The variation in criteria associated with an increase in the state of knowledge or change in the level of acceptability is also discussed.
INTRODUCTION

Acceptable risk lies at the heart of all technological decision making since the future is uncertain and there is no guarantee of absolute safety with any design. Although the operational decisions are technological, the definition of acceptable risk is a human decision.

This paper focuses on the probabilistic scientific principles associated with acceptable risk decisions involving nuclear power plants. The methodology employs Bayesian statistical decision concepts.

Uncertainties are found in problem assessments such as with natural and human hazards, in the properties of natural and engineered materials and their assembly, in the future performances of engineered designs and consequences of their performances, in the regulatory decision environment, and in a wide variety of economic and social factors which interact with technological decisions. The position of acceptable risk decision making is shown in Figure 1. Note that the acceptable risk decision itself must be deterministic in nature while all the input to this decision involves uncertainty.

VALUE

Value is the least understood and perhaps the single most important ingredient in acceptable risk decision making. There exists no general agreement upon theory of value or methodology to analyze values, particularly in the area of technological decision making. In fact, many engineers and scientists either deny the existence of value by acting "objectively" or fail to identify the role of value in recommendations. It is assumed in this paper that decisions are made because value exists and that decision makers receive value as a consequence of these decisions. Thus the optimum decision is that associated with receipt of the largest value to the decision maker. Conversely, an action that has been taken must have been associated with the expected receipt of maximum value. Note that value is most often subjective rather than objective and value can be transferred from one human to another. The essence of professionalism is found in the transfer of subjective values from the client to the professional.

The simplest decision situation is shown in Figure 2, in which the decision maker must choose one of the two actions, a₁ or a₂, after which the future can include the occurrence of a major hazard, and the decision maker will then receive value depending on the action taken and the future that is experienced. The probability measures, \( P = ( ) \), effectively provide weights on the occurrence of the two possible future events as well as the associated values, much as in a game of chance.

Obviously, the optimum decision depends on the possible actions, the probabilities, and the values to the decision maker. Once these are established, the hazard itself has nothing to do with the decision. The possible actions are given by the problem situation and the probability measures are objectively defined by the hazard. There can be great variability in the assessment of these probability measures. In fact, they
often tend to get confused with values, particularly after a bad experience. That is, receipt of a bad outcome can have the apparent influence of an increase in probability of occurrence of that outcome.

The values shown are single gamble values, estimates for this single decision. Values are estimates made by the decision maker at the time of decision making. A convenient technique in value assessment is shown in Table 1, in which possible values and their probability of receipt for $a_1$ are shown with the sum of the products being used as the summary statistic.

The optimum decision is obtained by folding back the decision tree by calculating the sum of the products of probability measures and values for each branching point. The expected values found are shown at the branching points so that 8.9 and -1.0 are to be compared in making the decision. For the example shown in Figure 2, action $a_1$ is optimum.

The influence of different decision makers can be seen in Figure 2 by noting that the values shown might fit an engineer or a manager accustomed to accepting risks. If the decision maker is a regulatory agency, the possible failure due to an extreme wind may be more important than the added cost of a more conservative design. The optimum decision easily becomes $a_2$ with changes in value. It is common for regulatory decision makers to refuse to recognize probability measures and choose the action based on the action with the smallest maximum loss, assuming that the worst possible event is certain to occur. This is the minimax decision rule. The expected value rule is employed in Figure 2.

3. HAZARDS

The decision tree of Figure 2 is concerned with a single hazard. A power plant is subject to many hazards, both natural and human, and the optimum overall system design is desired. A practical methodology for making assessments leading to acceptable risk decisions with multiple hazards has been discussed in Benjamin, Shah, and Shinozuka [1] and Benjamin and Kost [2]. Bosshard [3] considers a wide variety of modeling techniques.

If the occurrence of the hazard is a discrete rare event such as an earthquake, pipe break, fire control failure, etc., the simplest approach is to use the actuarial annual rate of occurrence to forecast future event relationships.

If the probability of event occurrence in any year is $p$, the probability of nonoccurrence is $1-p$, so that the probability of nonoccurrence for $n$ consecutive years is $(1-p)^n$ and the probability of at least one occurrence in $n$ years is $1-(1-p)^n$. If the probability of occurrence in any year is small, the probability of at least one occurrence in $n$ years is approximately $np$. If there is uncertainty about the value of $p$ because of very few events being observed, the probability of $x_1$ occurrences and $x_2$ nonoccurrences in $n$ years, given the history of $x_1$ occurrences and $x_2$ nonoccurrences in $n$ years, is given by the Bayesian Forecast as discussed in Benjamin and Cornell [4]:
\[ P(x'_1, x'_2|x_1, x_2) = \frac{n_0! (n+1)! (x_1+x'_1)! (x_2+x'_2)!}{x'_1! x'_1! x_1! x_2! (n+n_0+1)!} \] (1)

As an example, assume one failure has been observed in 100 operation years. What is the probability of one or more failures in the next 100 operation years, or in the next 1,000 years?

If the probability of occurrence is estimated to be \( 1/100 = 0.01 \), the probability of at least one failure in the next 100 years is

\[ 1 - (1-0.01)^{100} = 0.63 \] (2)

In 1,000 years of operation it is \( 1-(1-0.01)^{1000} = 0.999996 \).

If the Bayesian relationship is employed, the probability of zero failures and 100 nonfailures is

\[ x'_1 = 0, \quad x'_2 = 100, \quad n_0 = 100 \\
 x_1 = 1, \quad x_2 = 99, \quad n = 100 \]

\[ P(0,100|1,99) = \frac{100!}{0!\ 100!\ 1!\ 99!\ 200!} = 0.25 \] (3)

Thus, the probability of at least one failure in the next 100 years is more correctly \( 1 - 0.25 = 0.75 \) rather than 0.63. It is generally true that actuarial forecasts based on minimal data yield probabilities of rare event occurrences which are too small. Note that if the record had been no failures in the past 100 years, the actuarial forecast would be no failures in the next 100 years, while the Bayesian forecast would be calculated as

\[ P(0,100|0,100) = \frac{100!}{0!\ 100!\ 0!\ 100!\ 200!} = 0.50 \] (4)

Thus the probability of at least one failure in the next 100 years is \( 1 - 0.50 = 0.50 \) and not zero.

Now, if the joint occurrence of two types of events whose occurrences are independent is desired, and each has a history of one event in 100 years over a long time span, the probability of both occurring in the next 100 years is \( (0.63)^2 = 0.40 \). The probability of no events of either type in 100 years is \( (0.37)^2 = 0.13 \). Note that this is not the occurrence of the events at the same instant of time, but rather a counting of events in the 100 years.

The more common problem involves both level and time of occurrence, with a zero level being the same as nonoccurrence. Bosshard [3] discussed various probabilistic models of combined loads, but no general solutions exist. A rather simple, but practical solution can be found providing certain assumptions are satisfied. The need for restrictive assumptions arises from modeling problems when dependence between hazard levels in successive time steps is considered. The dependency problem can be solved
at a cost of considerable increase in mathematical complexity.

For a simple approximate solution, assume that time can be broken into a series of finite steps, that levels of events are independent between time steps, and that changes in level can only occur at the beginning and end of a time step. For example, if a fire has a duration of one hour and can be of level zero, one, or two and a control failure is similarly of one hour duration (same beginning and ending) with three possible levels, all possible conditions that can exist in any hour are shown in the sample space (Fig. 3).

For simplicity, assume first that the probability of the fire level is independent of control function. Each separate type of event can be described by a multinomial probability distribution and the joint distribution is joint multinomial in fprn. For simplicity, assume further that the zero state of each independent type of event has a probability of 0.9, the unit state has probability 0.09, and the second state has a probability of occurrence of 0.01. The probabilities of occurrence of the joint events are defined by the products of the marginal distributions, as shown in Figure 3. It is now a simple matter to compute the probability of any set of joint occurrences in any number of hours. For example, if the time span of interest is five hours, the probability of (0, 0) for five consecutive hours is equal to \((0.81)^5 = 0.35\), or a sequence (0, 0) for four hours followed by (2, 2) for one hour is \((0.81)^4(0.0001) = 0.000043\). The probability of four hours of (0, 0) and one hour of (1, 1) in any order is \((5)(0.0001)(0.81)^4 = 0.0174\). The factor of five appears in the last calculation since the desired combination can occur in five different ways.

An immediate practical application of the methodology to an acceptable risk problem is found with combinations of natural hazards. For example, consider flood and earthquake loads in which the latter type of event is equally likely to occur in any 30-second interval of time (duration is 30 seconds). Actual flow conditions are correlated from one 30-second interval to the next, but are not correlated with earthquake loads so that the correlation of flood levels is unimportant over long time spans. Assume that both hazards can be modeled as simple mixed probability distributions (Fig. 4). The continuous portion of the distributions are of the exponential type and give the probability of levels in intervals only. That is, the probability of an acceleration level exactly equal to 0.5g is zero, but the probability of an acceleration level equal to or larger than 0.5g is defined by the area under the continuous part of the distribution from 0.5g to infinity (see Fig. 4). The sample space defines all possible events. The joint probability distribution defines the probability of occurrence of all possible events, all levels of earthquake, including no earthquake, and all levels of flow, including no flow, in any 30-second interval.

Assume that the design level for earthquake alone is 0.5g and that the analysis of all the earthquake occurrence data has yielded the marginal probability density function shown for earthquake. A year contains
approximately \( 1 \times 10^6 \) intervals of 30 seconds. On an average, one earthquake a year is experienced and the mean effective peak ground acceleration is 0.1g. The probability that the acceleration will equal or exceed 0.5g in any earthquake is

\[ e^{-10}(0.5) = 0.0067 \]  

so that in 20 years the probability of an acceleration equal to or larger than 0.5g is \( 1-(1-0.0067)^{20} = 0.13 \).

Conventional flood data consist of the set of largest annual flows or annual peak flows. Such data are of no direct value in defining the flow level that exists in any 30-second interval. The data should consist rather of a random sample of the record of flow levels for each 30 seconds for a sufficient number of years to define the phenomena. The data will include samples of the peak flows as well as all other levels. That is, the annual peak flood level exists for only one time step in the year and while it is possible for an earthquake to occur in the same time step, it is much more likely that a flow level less than the peak value will be present at the time of an earthquake occurrence. The flow level that exists in any time step may be reasonably modeled by the exponential distribution shown in Figure 4. If flow at a level exists for seven days in each 365 on an average, the probability spike at zero level has a magnitude of \((365-7)/365 = 0.98\), so that the area of the continuous portion of the probability density function is \(1-0.98 = 0.02\). Assume that the mean height is one foot for all the 30-second steps in which the height is larger than zero. The probability distribution of flood level is then as shown in Figure 4.

The flood level with the same probability of exceedance in a 30-second time step as the 0.5g earthquake \((P = 6.74 \times 10^{-9})\) is found from

\[ (0.02)(e^{-y}) = 6.74 \times 10^{-9} \]

\[ y = 14.9 \text{ ft} \]

If earthquake and flood loads are associated with the same operational or safety consequence, the flood level of 14.9 feet is consistent with the 0.5g earthquake so that a design based on this set would be balanced for the hazards taken separately. Balance implies the same probability of exceedance and the same consequence associated with that exceedance.

The joint probability distribution for levels other than zero is defined by the product of the marginal distributions:

\[ f(x,y) = (0.02 \times 10^{-5})e^{-10x-y} \]

If \(10x+y\) is equal to a constant, all values of \(f(x,y)\) are constant, and all contour lines on the joint distribution are straight lines. If \(10x+y = 5\), a contour line from \(x = 0.5g\) to \(y = 5\) ft is defined. Each straight line or contour has the unique property of constant probability of joint load exceedance. To be consistent with the marginal design limits, the line \((defined \, by \, 10x+y = 1.09)\) defines all values of earthquake acceleration and flood level balanced with the marginal requirements of 0.5g and 14.9 ft. The balanced design is shown in Figure 5.
The situation chosen shows the great influence of the condition of exactly zero load for large portions of the time. If magnitudes of loads greater than zero exist all of the time and these magnitudes are defined by continuous probability distributions of exponential form, the joint loading for balanced design passes through the marginal design requirements (Fig. 5). If the probability distributions are normal, gamma, extreme value, or of that general shape, the desired balanced design contours are curved lines. Thus the combined loading requirements for balance, a desirable acceptable risk condition, are sensitive to the actual physical properties of the hazards.

The problem with making decisions on combined loadings for design criteria based on joint exceedance probabilities is illustrated in Figure 6, in which both hazards exist continuously in time and marginal requirements have led to \( x_1 \) and \( y_1 \) as design values for the hazards separately. If the exceedance probabilities of \( x_1 \) and \( y_1 \) are each 0.001 per year, should the design combined loading be \((x_1, y_1)\) or possibly \((0.5x_1, 0.5y_1)\)? If the marginal exceedance probabilities are multiplied, the probability of loads equal to or larger than \( x_1 \) and equal to or larger than \( y_1 \) is \( 10^{-6} \). This is the probability of loads in the double hatched area of Figure 6.

Can the combined load case \((x_1, y_1)\) be excluded on the basis of neglecting probabilities of failure of \( 10^{-6} \) and less per year? To answer this question, assume that Design 1 of Figure 6 is employed in which failure is acceptable for \( X > x_1 \), and for \( Y > y_1 \). Such a design does not have a probability of failure of \( 10^{-6} \) since all loads in the single and double hatched area are associated with acceptable failure. The probability of loads equal to or less than \( x_1 \) is 0.999 and less than \( y_1 \) is also 0.999, so that the joint occurrence of both is \((0.999)(0.999) = 0.998 \) and the true probability of failure is \( 1 - 0.998 = 0.002 \) and not \( 10^{-6} \).

More complex analyses of combined loadings have been made for particular problems and complications such as dependence and more than two hazards. Multiple consequences have also been rationally considered.

4. RELIABILITY

Reliability engineering is based on the assumption that the probability of failure of any component or system to function as designed is not zero under operating conditions. The probability of failure is thus greater than zero since the sum of the reliability and the probability of failure is equal to unity. If the design requirement is unit reliability, absolute safety, the extensive methodology and experience in reliability engineering cannot be rationally applied. Oddly enough, some specifications require both absolute safety and redundancy, which is only effective if the component reliability is less than unity. Reliabilities must be quantified goals in acceptable risk decisions. There also can be no absolute proof that a particular reliability goal has been attained by any design or performance, only inferences to that effect.
Simple reliability theory deals with systems classed as series, parallel, or mixed (compound). With series systems, all components must survive for the system to survive, the reliability of the system is equal to the product of the independent component reliabilities, the smallest reliability dominates the system, and the system reliability is less than the least component reliability. With parallel or redundant systems, a failure brings the redundant component into action; the reliability of the system is equal to unity minus the product of the independent probabilities of failure. With such systems, the system reliability is dominated by the parallel component with the largest reliability and the system reliability is larger than the largest component reliability. Note that simple reliability theory assumes that components either fail or survive and there exists perfect switching to the redundant component in the event of a failure.

With complex systems such as found in a nuclear power plant, simple reliability concepts do not generally fit the systems employed owing to complex response patterns such as partial failures and a lack of independence between component properties for a variety of reasons including response-loading interaction, multiple loadings, and the transient probabilistic nature of both loading and response. The importance of dependency between components in a redundant system is obvious, since perfect dependency says that if a component fails, its redundant component also fails. Even partial dependency greatly reduces systems reliability.

Structural systems generally do not fit simple reliability theory since these systems are both continuous and respond to complex multiple interactive probabilistic and transient loadings. Response depends on the loading and possibly on the time history of response up to that loading. Component properties as well as loadings are dependent. Despite these difficulties, a basic methodology has been developed that can solve these and other problems (Ang [5]).

5. INFLUENCE OF FORM OF ACCEPTABLE RISK CRITERIA

Acceptable risk criteria can have two basic forms. The common engineering form assumes that the criteria depends on the level of the hazard and is independent of the number of such hazards. Alternately, the societal rule says that the criteria changes with the characteristics of the aggregate consequences. The common engineering approach is to assume that if the first nuclear power plant is acceptable from the risk standpoint, another plant of the same design is acceptable. The societal rule aggregates the consequences of inadequate performance and examines this aggregate for acceptability. The engineering approach leads to standard designs, while the societal rule leads to "ratcheting" or the requirement that each succeeding design be more conservative than the last. With the societal rule, first-constructed designs can change from acceptable to not acceptable. Acceptability cannot be measured on an actuarial basis. The societal rule implies that the cost of failure is a function of the probability of failure, with cost increasing very rapidly as the likelihood
of failure increases.

The engineering form has led to a search for an acceptable probability of failure or an acceptable mean rate of accidents or human casualties on the basis of actuarial risk per plant. If, however, the consequence of inadequate performance depends on the probability of that performance, these searches for "objective" measures cannot succeed. For example, assume that the probability of core melt from internal malfunction with the first plant is estimated to be $10^{-6}$ per reactor year per unit and this is acceptable compared to a limit of $10^{-5}$. If now 100 more identical plants are placed in operation, the probability of core melt per year with these 100 plants is $(10^{-6})(10^2) = 10^{-4}$ per year, and in ten years of future operation, this probability becomes $10^{-3}$. Obviously there is a point with more and more plants in operation for long periods of time when the occurrence of at least one core melt is no longer associated with a very small probability measure. The engineering form of the acceptable risk rule would accept this forecast as a verification of the design. In contrast, societal reaction rule would force the retirement of old plants, or an assessment that the next new plant be constructed to a very much smaller probability of core melt owing to the existence of the older plants.

In effect, the societal rule takes the form of allowing one core melt in a given number of years regardless of the number of plants in operation. If this is the rule, each succeeding plant must be constructed with a smaller probability of malfunction until a limit is reached and new construction requires the retirement of the oldest plants. For example, assume that the acceptable probability of core melt in 50 years from all plants is $Q$, that of the first plant is $Q/2$ in 50 years, and the acceptable probability for a second plant is $B$.

$$P[\text{No failure from first plant}] = 1 - Q/2$$
$$P[\text{No failure from second plant}] = 1 - B$$
$$P[\text{No failure in either plant}] = (1-Q/2)(1-B)$$
$$P[\text{One or more failures, both plants}] = 1 - (1-Q/2)(1-B)$$
$$1 - (1-Q/2)(1-B) = Q$$
$$B = Q/(2-Q)$$

Thus $B$ is very nearly $Q/2$. With three or more reactors, the condition that the simple sum of the probabilities of failure cannot exceed $Q$ is a close approximation.

6. Equivalence

Problems involving equivalence can arise either in the form of changes of standards or in comparisons between facilities. Both situations are examined briefly in this section.

Changes in standards very often cannot be directly approached by direct compliance at reasonable cost so that the issue becomes the equivalence of performance of an upgraded system with a different system which has now become a standard. If there is no difference between the systems in terms
of consequences of failure to perform, the systems are equivalent if the two reliabilities are the same. If \( R_0 \) is the reliability of the old system without modifications and \( R_n \) is the reliability with the new standard, the problem of concern involves

\[ R_n > R_0 \]

In terms of systems configurations, addition of a component in series with the existing components cannot increase the reliability. In the simplest form, the new component must either add effective redundancy or provide additive capacity. If the problem is inadequate strength of a member, redundancy implies the placement of an additional member such that the new member is only effective upon failure of the original member. Obviously, to be effective the new member must not be likely to fail if the original member fails from the same flaw, for example. The event tree of Figure 7 shows the system. Note that a sequence of function is implied.

The more common situation is that of adding capacity. If no change in response characteristics or consequences is involved, this is simple compliance. Frequently, the addition of a strengthening element reduces the reliability or capacity of the original element. The assumption is that of additive capacity in which the new mean capacity is equal to the sum of the effective mean capacities. The variability of capacity changes at the same time depending on the correlation between capacities.

To illustrate another type of problem, assume that two nuclear reactors are to be built in two different geological environments, but are to start operation at the same time and coincident with the shutdown of an old reactor. The two reactors can be designed to different equivalence restrictions. First, their lifetime expected losses may be required to be equal, and, second, the societal restriction that the total annual expected loss for all reactors in operation must remain at or below a specified small quantity \( Q \). The two restrictions can be written as

1. \( E[\text{lifetime loss reactor 1}] = E[\text{lifetime loss reactor 2}] \)
2. \( \text{Total } E[\text{annual loss of all operating reactors}] \leq Q \)

These or similar relationships can be employed to ensure satisfaction of acceptable risk criteria in terms of parameters directly related to design.

7. CONCLUSION

Although philosophical questions dealing with acceptable risk as a human problem are beyond the scope of this paper, it is appropriate to point out that probabilistic analyses of the type discussed cannot be fully definitive. Only a portion of human wisdom can be quantified and treated mathematically. In terms of a simple decision of the type shown in Figure 2, other options and future conditions of nature can exist and other values can exist. Thus it is possible that the true optimum decision can differ from that indicated by mathematics alone.

This does not mean that analyses should not be made, but rather that the results must be treated with judgment. Note further that the optimum
decision can be associated with a bad outcome, so that the measure of utility of the methodology requires a long run viewpoint.

References


3. BOSSHARD, W., "On Stochastic Load Combination," Report No. 16, John A. Blume Earthquake Engineering Center, Department of Civil Engineering, Stanford University, July 1975.


<table>
<thead>
<tr>
<th>Value</th>
<th>Probability</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.909</td>
<td>0</td>
</tr>
<tr>
<td>-1,000</td>
<td>0.090</td>
<td>-90</td>
</tr>
<tr>
<td>-10,000</td>
<td>0.001</td>
<td>-10</td>
</tr>
<tr>
<td>Sum</td>
<td>1.000</td>
<td>-100</td>
</tr>
</tbody>
</table>

Summary Statistic = -100
Figure 1 Components of Acceptable Risk Decision, Certainty in an Uncertain World

Figure 2 Simple Decision Tree
Figure 3  Sample Space and Joint Probabilities

Figure 4  Joint Occurrence Model

Figure 5  Joint Occurrence Situations
Figure 6 Criteria Conditions

Figure 7 Event Tree for Equivalence