Basic Risk Concepts

1.1 INTRODUCTION

Risk assessment and risk management are two separate but closely related activities. The fundamental aspects of these two activities are described in this chapter, which provides an introduction to subsequent developments. Section 1.2 presents a formal definition of risk with focus on the assessment and management phases. Sources of debate in current risk studies are described in Section 1.3. Most people perform a risk study to avoid serious mishaps. This is called risk aversion, which is a kernel of risk management; Section 1.4 describes risk aversion. Management requires goals; achievement of goals is checked by assessment. An overview of safety goals is given in Section 1.5.

1.2 FORMAL DEFINITION OF RISK

Risk is a word with various implications. Some people define risk differently from others. This disagreement causes serious confusion in the field of risk assessment and management. The Webster’s Collegiate Dictionary, 5th edition, for instance, defines risk as the chance of loss, the degree of probability of loss, the amount of possible loss, the type of loss that an insurance policy covers, and so forth. Dictionary definitions such as these are not sufficiently precise for risk assessment and management. This section provides a formal definition of risk.

1.2.1 Outcomes and Likelihoods

Astronomers can calculate future movements of planets and tell exactly when the next solar eclipse will occur. Psychics of the Delphi Temple of Apollo foretold the future by divine inspiration. These are rare exceptions, however. Just as a TV weatherperson, most
people can only forecast or predict the future with considerable uncertainty. Risk is a concept attributable to future uncertainty.

**Primary definition of risk.** A weather forecast such as "30 percent chance of rain tomorrow" gives two outcomes together with their likelihoods: (30%, rain) and (70%, no rain). Risk is defined as a collection of such pairs of likelihoods and outcomes:

\[ \{(30\%, \text{rain}), (70\%, \text{no rain})\}. \]

More generally, assume \( n \) potential outcomes in the doubtful future. Then risk is defined as a collection of pairs.

\[
\text{Risk} = \{(L_1, O_1), \ldots, (L_i, O_i), \ldots, (L_n, O_n)\}
\]

(1.1)

where \( O_i \) and \( L_i \) denote outcome \( i \) and its likelihood, respectively. Throwing a die yields the risk,

\[
\text{Risk} = \{\left(\frac{1}{6}, 1\right), \left(\frac{1}{6}, 2\right), \ldots, \left(\frac{1}{6}, 6\right)\}
\]

(1.2)

where the outcome is a particular face and the likelihood is probability 1 in 6.

In situations involving random chance, each face involves a beneficial or a harmful event as an ultimate outcome. When the faces are replaced by these outcomes, the risk of throwing the die can be rewritten more explicitly as

\[
\text{Risk} = \{\left(\frac{1}{6}, 0\right), \left(\frac{1}{6}, -1\right), \ldots, \left(\frac{1}{6}, -6\right)\}
\]

(1.3)

**Risk profile.** The distribution pattern of the likelihood-outcome pair is called a risk profile (or a risk curve); likelihoods and outcomes are displayed along vertical and horizontal axes, respectively. Figure 1.1 shows a simple risk profile for the weather forecast described earlier: two discrete outcomes are observed along with their likelihoods, 30% rain or 70% no rain.

In some cases, outcomes are measured by a continuous scale, or the outcomes are so many that they may be continuous rather than discrete. Consider an investment problem where each outcome is a monetary return (gain or loss) and each likelihood is a density of experiencing a particular return. Potential pairs of likelihoods and outcomes then form a continuous profile. Figure 1.2 is a density profile where a positive or a negative amount of money indicates loss or gain, respectively.

**Objective versus subjective likelihood.** In a perfect risk profile, each likelihood is expressed as an objective probability, percentage, or density per action or per unit time, or during a specified time interval (see Table 1.1). Objective frequencies such as two occurrences per year and ratios such as one occurrence in one million are also likelihoods; if the frequency is sufficiently small, it can be regarded as a probability or a ratio. Unfortunately, the likelihood is not always exact; probability, percentage, frequency, and ratios may be based on subjective evaluation. Verbal probabilities such as rare, possible, plausible, and frequent are also used.

---

*To avoid proliferation of technical terms, a hazard or a danger is defined in this book as a particular process leading to an undesirable outcome. Risk is a whole distribution pattern of outcomes and likelihoods; different hazards may constitute the risk "fatality," that is, various natural or man-made phenomena may cause fatalities through a variety of processes. The hazard or danger is akin to a causal scenario, and is a more elementary concept than risk.*
Figure 1.1. Simple risk profile from a weather forecast.

Figure 1.2. Occurrence density and complementary cumulative risk profile.
### TABLE 1.1. Examples of Likelihood and Outcome

<table>
<thead>
<tr>
<th>Likelihood Measure</th>
<th>Unit</th>
<th>Outcome Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability</td>
<td>Per Action</td>
<td>Physical</td>
</tr>
<tr>
<td>Percentage</td>
<td>Per Demand or Operation</td>
<td>Physiological</td>
</tr>
<tr>
<td>Density</td>
<td>Per Unit Time</td>
<td>Psychological</td>
</tr>
<tr>
<td>Frequency</td>
<td>During Lifetime</td>
<td>Financial</td>
</tr>
<tr>
<td>Ratio</td>
<td>During Time Interval</td>
<td>Time, Opportunity</td>
</tr>
<tr>
<td>Verbal Expression</td>
<td>Per Mileage</td>
<td>Societal, Political</td>
</tr>
</tbody>
</table>

**Complementary cumulative profile.** The risk profile (discrete or continuous) is often displayed in terms of complementary cumulative likelihoods. For instance, the likelihood $F(x) = \int_x^\infty f(u)du$ of losing $x$ or more money is displayed rather than the density $f(x)$ of just losing $x$. The second graph of Figure 1.2 shows a complementary cumulative risk profile obtained from the density profile shown by the first graph. Point $P$ on the vertical axis denotes the probability of losing zero or more money, that is, a probability of not getting any profit. The complementary cumulative likelihood is a monotonously decreasing function of variable $x$, and hence has a simpler shape than the density function. The complementary representation is informative because decision makers are more interested in the likelihood of losing $x$ or more money than in just $x$ amount of money; for instance, they want to know the probability of “no monetary gain,” denoted by point $P$ in the second graph of Figure 1.2.

**Farmer curves.** Figure 1.3 shows a famous example from the Reactor Safety Study [1] where annual frequencies of $x$ or more early fatalities caused by 100 nuclear power plants are predicted and compared with fatal frequencies by air crashes, fires, dam failures, explosions, chlorine releases, and air crashes. Nonnuclear frequencies are normalized by a size of population potentially affected by the 100 nuclear power plants; these are not frequencies observed on a worldwide scale. Each profile in Figure 1.3 is called a Farmer curve [2]; horizontal and vertical axes generally denote the accident severity and complementary cumulative frequency per unit time, respectively.

Only fatalities greater than or equal to 10 are displayed in Figure 1.3. This is an exceptional case. Fatalities usually start with unity; in actual risk problems, a zero fatality has a far larger frequency than positive fatalities. Inclusion of a zero fatality in the Farmer curve requires the display of an unreasonably wide range of likelihoods.

### 1.2.2 Uncertainty and Meta-Uncertainty

**Uncertainty.** A kernel element of risk is uncertainty represented by plural outcomes and their future likelihoods. This point is emphasized by considering cases without uncertainty.

**Outcome guaranteed.** No risk exists if the future outcome is uniquely known (i.e., $n = 1$) and hence guaranteed. We will all die some day. The probability is equal to 1, so there would be no fatal risk if a sufficiently long time frame is assumed. The rain risk does not exist if there was 100% assurance of rain tomorrow, although there would be other risks such as floods and mudslides induced by the rain. In a formal sense, any risk exists if and only if more than one outcome ($n \geq 2$) are involved with positive likelihoods during a specified future time interval. In this context, a situation with two opposite outcomes with
equal likelihoods may be the most risky one. In less formal usage, however, a situation is called more risky when severities (or levels) of negative outcomes or their likelihoods become larger; an extreme case would be the certain occurrence of a negative outcome.

**Outcome localized.** A $10^{-6}$ lifetime likelihood of a fatal accident to the U.S. population of 236 million implies 236 additional deaths over an average lifetime (a 70-year interval). The 236 deaths may be viewed as an acceptable risk in comparison to the 2 million annual deaths in the United States [3].

\[
\text{Risk} = (10^{-6}, \text{fatality}) : \text{acceptable} \quad (1.4)
\]

On the other hand, suppose that 236 deaths by cancer of all workers in a factory are caused, during a lifetime, by some chemical intermediary totally confined to the factory and never released into the environment. This number of deaths completely localized in the
factory is not a risk in the usual sense. Although the ratio of fatalities in the U.S. population remains unchanged, that is, $10^{-6}$/lifetime, the entire U.S. population is no longer suitable as a group of people exposed to the risk: the population should be replaced by the group of people in the factory.

$$\text{Risk} = (1, \text{fatality}) : \text{unacceptable} \quad (1.5)$$

Thus a source of uncertainty inherent to the risk lies in the anonymity of the victims. If the names of victims were known in advance, the cause of the outcome would be a crime. Even though the number of victims (about 11,000 by traffic accidents in Japan) can be predicted in advance, the victims' names must remain unknown for risk problem formulation purposes.

If only one person is the potential victim at risk, the likelihood must be smaller than unity. Assume that a person living alone has a defective staircase in his house. Then only one person is exposed to a possible injury caused by the staircase. The population affected by this risk consists of only one individual: the name of the individual is known and anonymity is lost. The injury occurs with a small likelihood and the risk concept still holds.

**Outcome realized.** There is also no risk after the time point when an outcome is realized. The airplane risk for an individual passenger disappears after the landing or crash, although he or she, if alive, now faces other risks such as automobile accidents. The uncertainty in the risk exists at the prediction stage and before its realization.

**Meta-uncertainty.** The risk profile itself often has associated uncertainties that are called meta-uncertainties. A subjective estimate of uncertainties for a complementary cumulative likelihood was carried out by the authors of the Limerick Study [4]. Their result is shown in Figure 1.4. The range of uncertainty stretches over three orders of magnitude. This is a fair reflection on the present state of the art of risk assessment. The error bands are a result of two types of meta-uncertainties: uncertainty in outcome level of an accident and uncertainty in frequency of the accident. The existence of this meta-uncertainty makes risk management or decision making under risk difficult and controversial.

In summary, an ordinary situation with risk implies uncertainty due to plural outcomes with positive likelihoods, anonymity of victims, and prediction before realization. Moreover, the risk itself is associated with meta-uncertainty.

### 1.2.3 Risk Assessment and Management

**Risk assessment.** A principal purpose of risk assessment is the derivation of risk profiles posed by a given situation: the weatherman performed a risk assessment when he promulgated the risk profile in Figure 1.1. The Farmer curves in Figures 1.3 and 1.4 are final products of a methodology called probabilistic risk assessment (PRA), which, among other things, enumerates outcomes and quantifies their likelihoods.

For nuclear power plants, the PRA proceeds as follows: enumeration of sequences of events that could produce a core melt; clarification of containment failure modes, their probabilities and timing; identification of quantity and chemical form of radioactivity released if the containment is breached; modeling of dispersion of radionuclides in the atmosphere; modeling of emergency response effectiveness involving sheltering, evacuation, and medical treatment; and dose-response modeling in estimating health effects on the population exposed [5].
**Risk management.** Risk management proposes alternatives, evaluates (for each alternative) the risk profile, makes safety decisions, chooses satisfactory alternatives to control the risk, and exercises corrective actions.*

**Assessment versus management.** When risk management is performed in relation to a PRA, the two activities are called a probabilistic risk assessment and management (PRAM). This book focuses on PRAM.

The probabilistic risk assessment phase is more scientific, technical, formal, quantitative, and objective than the management phase, which involves value judgment and heuristics, and hence is more subjective, qualitative, societal, and political. Ideally, the PRA is based on objective likelihoods such as electric bulb failure rates inferred from statistical data and theories. However, the PRA is often compelled to use subjective likelihoods based on intuition, expertise, and partial, defective, or deceitful data, and dubious theories. These constitute the major source of meta-uncertainty in the risk profile.

Considerable efforts are being made to establish a unified and scientific PRAM methodology where subjective assessment, value judgment, expertise, and heuristics are dealt with more objectively. Nonetheless the subjective or human dimension does constitute one of the two pillars that support the entire conceptual edifice [3].

*Terms such as *risk estimation* and *risk evaluation* only cause confusion, and should be avoided.*
1.2.4 Alternatives and Controllability of Risk

Example 1—Daily risks. An interesting perspective on the risks of our daily activity was developed by Imperial Chemical Industries Ltd. [6]. The ordinate of Figure 1.5 is the fatal accident frequency rate (FAFR), the average number of deaths by accidents in 10^8 hours of a particular activity. An FAFR of unity corresponds to one fatality in 11,415 years, or 87.6 fatalities per one million years. Thus a motor driver according to Figure 1.5 would, on the average, encounter a fatal accident if she drove continuously 17 years and 4 months, while a chemical industry worker requires more than 3000 years for his fatality.

![Diagram showing fatal accident frequency rates of daily activities.

Key
a: Sleeping time
b: Eating, washing, dressing, etc., at home
c: Driving to or from work by car
d: The day's work
e: The lunch break
f: Motorcycling
g: Commercial entertainment

Figure 1.5. Fatal accident frequency rates of daily activities.

Risk control. The potential for plural outcomes and single realization by chance recur endlessly throughout our lives. This recursion is a source of diversity in human affairs. Our lives would be monotonous if future outcomes were unique at birth and there were no risks at all; this book would be useless too. Fortunately, enough or even an excessive amount of risk surrounds us. Many people try to assess and manage risks; some succeed and others fail.
Active versus passive controllability. Although the weatherperson performs a risk assessment, he cannot alter the likelihood, because rain is an uncontrollable natural phenomenon. However, he can perform a risk management together with the assessment; he can passively control or mitigate the rain hazard by suggesting that people take an umbrella; the outcome “rain” can be mitigated to “rain with umbrella.”

Figure 1.5 shows seven sources (a to g) of the fatality risk. PRA deals with risks of human activities and systems found in engineering, economics, medicine, and so forth, where likelihoods of some outcomes can be controlled by active intervention, in addition to the passive mitigation of other outcomes.

Alternatives and controllability. Active or passive controllability of risks inherently assumes that each alternative chosen by a decision maker during the risk-management phase has a specific risk profile. A baseline decision or action is also an alternative. In some cases, only the baseline alternative is available, and no room is left for choice. For instance, if an umbrella is not available, people would go out without it. Similarly, passengers in a commercial airplane flying at 33,000 feet have only the one alternative of continuing the flight. In these cases, the risk is uncontrollable. Some alternatives have no appreciable effect on the risk profile, while others bring desired effects; some are more cost effective than others.

Example 2—Alternatives for rain hazard mitigation. Figure 1.6 shows a simple tree for the rain hazard mitigation problem. Two alternatives exist: 1) going out with an umbrella (A₁), and 2) going out without an umbrella (A₂). Four outcomes are observed: 1) O₁₁ = rain, with umbrella; 2) O₁₂ = no rain, with umbrella; 3) O₁₂ = rain, without umbrella; and 4) O₁₂ = no rain, without umbrella. The second subscript denotes a particular alternative, and the first a specific outcome under the alternative. In this simple example, the rain hazard is mitigated by the umbrella, though the likelihood (30%) of rain remains unchanged. Two different risk profiles appear, depending on the alternative chosen, where R₁ and R₂ denote the risks with and without the umbrella, respectively:

\[ R_1 = \{(30\%, O_{11}), (70\%, O_{12})\} \quad (1.6) \]

\[ R_2 = \{(30\%, O_{12}), (70\%, O_{22})\} \quad (1.7) \]

Figure 1.6. Simple branching tree for rain hazard mitigation problem.
In general, a choice of particular alternative \( A_j \) yields risk profile \( R_j \) where likelihood \( L_{ij} \), outcome \( O_{ij} \), and total number \( n_j \) of outcomes vary from alternative to alternative:

\[
R_j = \{ (L_{ij}, O_{ij}) \mid i = 1, \ldots, n_j \}, \quad j = 1, \ldots, m
\]  

(1.8)

The subscript \( j \) denotes a particular alternative. This representation denotes an explicit dependence of the risk profile on the alternative.

Choices and alternatives exist in almost every activity: product design, manufacture, test, maintenance, personnel management, finance, commerce, health care, leisure, and so on. In the rain hazard mitigation problem in Figure 1.6, only outcomes could be modified. In risk control problems for engineering systems, both likelihoods and outcomes may be modified, for instance, by improving plant designs and operation and maintenance procedures. Operating the plant without modification or closing the operation are also alternatives.

**Outcome matrix.** A baseline risk profile changes to a new one when a different alternative is chosen. For the rain hazard mitigation problem, two sets of outcomes exist, as shown in Table 1.2. The matrix showing the relation between the alternative and outcome is called an outcome matrix. The column labeled utility will be described later.

### TABLE 1.2. Outcome Matrix of Rain Hazard Mitigation Problem

<table>
<thead>
<tr>
<th>Alternative</th>
<th>Likelihood</th>
<th>Outcome</th>
<th>Utility</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A_1 ): With umbrella</td>
<td>( L_{11} = 30% )</td>
<td>( O_{11}: ) Rain, with umbrella</td>
<td>( U_{11} = 1 )</td>
</tr>
<tr>
<td>( A_1 ): With umbrella</td>
<td>( L_{21} = 70% )</td>
<td>( O_{21}: ) No rain, with umbrella</td>
<td>( U_{21} = 0.5 )</td>
</tr>
<tr>
<td>( A_2 ): Without umbrella</td>
<td>( L_{12} = 30% )</td>
<td>( O_{12}: ) Rain, without umbrella</td>
<td>( U_{12} = 0 )</td>
</tr>
<tr>
<td>( A_2 ): Without umbrella</td>
<td>( L_{22} = 70% )</td>
<td>( O_{22}: ) No rain, without umbrella</td>
<td>( U_{22} = 1 )</td>
</tr>
</tbody>
</table>

**Lotteries.** Assume that \( m \) alternatives are available. The choice of alternative \( A_j \) is nothing but a choice of lottery \( R_j \) among the \( m \) lotteries, the term lottery being used to indicate a general probabilistic set of outcomes. Two lotteries, \( R_1 \) and \( R_2 \), are available for the rain hazard mitigation problem in Figure 1.6; each lottery yields a particular statistical outcome. There is a one-to-one correspondence among risk, risk profile, lottery, and alternative; these terms may be used interchangeably.

**Risk-free alternatives.** Figure 1.7 shows another situation with two exclusive alternatives \( A_1 \) and \( A_2 \). When alternative \( A_1 \) is chosen, there is a fifty-fifty chance of losing $1000 or nothing; the expected loss is \((1000 \times 0.5) + (0 \times 0.5) = $500\). The second alternative causes a certain loss of $500. In other words, only one outcome can occur when alternative \( A_2 \) is chosen; this is a risk-free alternative, as a payment for accident insurance to compensate for the $1000 loss that occurs with probability 0.5. Alternative \( A_1 \) has two outcomes and is riskier than alternative \( A_2 \) because of the potential of the large $1000 loss.

It is generally believed that most people prefer a certain loss to the same amount of expected loss; that is, they will buy insurance for $500 to avoid lottery \( R_1 \). This attitude is called risk aversion: they would not buy insurance, however, if the payment is more than $750, because the payment becomes considerably larger than the expected loss.
Sec. 1.2  ■  Formal Definition of Risk

Some people seek thrills and expose themselves to the first lottery without buying the $500 insurance; this attitude is called risk seeking or risk prone. Some may buy insurance if the payment is, for instance, $250 or less, because the payment is now considerably smaller than the expected loss.

The risk-free alternative is often used as a reference point in evaluating risky alternatives like lottery $R_1$. In other words, the risky alternative is evaluated by how people trade it off with a risk-free alternative that has a fixed amount of gain or loss, as would be provided by an insurance policy.

**Alternatives as barriers.** The MORT (management oversight and risk tree) technique considers injuries, fatalities, and physical damage caused by an unwanted release of energy whose forms may be kinetic, potential, chemical, thermal, electrical, ionizing radiation, non-ionizing radiation, acoustic, or biologic. Typical alternatives for controlling the risks are called barriers in MORT [7] and are listed in Table 1.3.

**TABLE 1.3.** Typical Alternatives for Risk Control

<table>
<thead>
<tr>
<th>Barriers</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Limit the energy (or substitute a safer form)</td>
<td>Low voltage instruments, safer solvents, quantity limitation</td>
</tr>
<tr>
<td>2. Prevent build-up</td>
<td>Limit controls, fuses, gas detectors, floor loading</td>
</tr>
<tr>
<td>3. Prevent the release</td>
<td>Containment, insulation</td>
</tr>
<tr>
<td>4. Provide for slow release</td>
<td>Rupture disc, safety valve, seat belts, shock absorption</td>
</tr>
<tr>
<td>5. Channel the release away, that is, separate in time or space</td>
<td>Roping off areas, aisle marking, electrical grounding, lockouts, interlocks</td>
</tr>
<tr>
<td>6. Put a barrier on the energy source</td>
<td>Sprinklers, filters, acoustic treatment</td>
</tr>
<tr>
<td>7. Put a barrier between the energy source and men or objects</td>
<td>Fire doors, welding shields</td>
</tr>
<tr>
<td>8. Put a barrier on the man or object to block or attenuate the energy</td>
<td>Shoes, hard hats, gloves, respirators, heavy protectors</td>
</tr>
<tr>
<td>9. Raise the injury or damage threshold</td>
<td>Selection, acclimatization to heat or cold</td>
</tr>
<tr>
<td>10. Treat or repair</td>
<td>Emergency showers, transfer to low radiation job, rescue, emergency medical care</td>
</tr>
<tr>
<td>11. Rehabilitate</td>
<td>Relaxation, recreation, recuperation</td>
</tr>
</tbody>
</table>
Cost of alternatives. The costs of life-saving alternatives in dollars per life saved have been estimated and appear in Table 1.4 [5]. Improved medical X-ray equipment requires $3600, while home kidney dialysis requires $530,000. A choice of alternative is sometimes made through a risk-cost-benefit (RCB) or risk-cost (RC) analysis. For an automobile, where there is a risk of a traffic accident, a seat belt or an air bag adds costs but saves lives.

TABLE 1.4. Cost Estimates for Life-saving Alternatives in Dollars per Life Saved

<table>
<thead>
<tr>
<th>Risk Reduction Alternatives</th>
<th>Estimated Cost (Dollars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Improved medical X-ray equipment</td>
<td>3,600</td>
</tr>
<tr>
<td>2. Improved highway maintenance practices</td>
<td>20,000</td>
</tr>
<tr>
<td>3. Screening for cervical cancer</td>
<td>30,000</td>
</tr>
<tr>
<td>4. Proctoscopy for colon/rectal cancer</td>
<td>30,000</td>
</tr>
<tr>
<td>5. Mobile cardiac emergency unit</td>
<td>30,000</td>
</tr>
<tr>
<td>6. Road guardrail improvements</td>
<td>30,000</td>
</tr>
<tr>
<td>7. Tuberculosis control</td>
<td>40,000</td>
</tr>
<tr>
<td>8. Road skid resistance</td>
<td>40,000</td>
</tr>
<tr>
<td>9. Road rescue helicopters</td>
<td>70,000</td>
</tr>
<tr>
<td>10. Screening for lung cancer</td>
<td>70,000</td>
</tr>
<tr>
<td>11. Screening for breast cancer</td>
<td>80,000</td>
</tr>
<tr>
<td>12. Automobile driver education</td>
<td>90,000</td>
</tr>
<tr>
<td>13. Impact-absorbing roadside device</td>
<td>110,000</td>
</tr>
<tr>
<td>14. Breakaway signs and lighting posts</td>
<td>120,000</td>
</tr>
<tr>
<td>15. Smoke alarms in homes</td>
<td>240,000</td>
</tr>
<tr>
<td>16. Road median barrier improvements</td>
<td>230,000</td>
</tr>
<tr>
<td>17. Tire inspection</td>
<td>400,000</td>
</tr>
<tr>
<td>18. Highway rescue cars</td>
<td>420,000</td>
</tr>
<tr>
<td>19. Home kidney dialysis</td>
<td>530,000</td>
</tr>
</tbody>
</table>

1.2.5 Outcome Significance

Significance of outcome. The significance of each outcome from each alternative must be evaluated in terms of an amount of gain or loss if an optimal and satisfactory alternative is to be chosen. Significance varies directly with loss and inversely with gain. An inverse measure of the significance is called a utility, or value function (see Table 1.5).* In PRA, the outcome and significance are sometimes called a consequence and a magnitude, respectively, especially when loss outcomes such as property damage and fatality are considered.

Example 3—Rain hazard decision-making problem. Assume that the hypothetical outcome utilities in Table 1.2 apply for the problem of rain hazard mitigation. The two outcomes “O_{11}: rain, with umbrella” and “O_{22}: no rain, without umbrella” are equally preferable and scored as unity. A less preferable outcome is “O_{21}: no rain, with umbrella” scored as 0.5. Outcome “O_{12}: rain, without umbrella” is least preferable with a score of zero. These utility values are defined for

*The significance, utility, or value are formal, nonlinear measures for representing outcome severity. The significance of two fatalities is not necessarily equal to twice the single fatality significance. Proportional measures such as lost money, lost time, and number of fatalities are often used for practical applications without nonlinear value judgments.
TABLE 1.5. Examples of Outcome Severity and Risk Level Measure

<table>
<thead>
<tr>
<th>Outcome Severity Measure</th>
<th>Risk Level Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significance</td>
<td>Expected significance</td>
</tr>
<tr>
<td>Utility, value</td>
<td>Expected utility or value</td>
</tr>
<tr>
<td>Lost money</td>
<td>Expected money loss</td>
</tr>
<tr>
<td>Fatalities</td>
<td>Expected fatalities</td>
</tr>
<tr>
<td>Longevity loss</td>
<td>Expected longevity loss</td>
</tr>
<tr>
<td>Dose</td>
<td>Expected outcome severity</td>
</tr>
<tr>
<td>Concentration</td>
<td>Severity for fixed outcome</td>
</tr>
<tr>
<td>Lost time</td>
<td>Likelihood for fixed outcome</td>
</tr>
</tbody>
</table>

outcomes, not for the risk profile of each alternative. As shown in Figure 1.8, it is necessary to create a utility value (or a significance value) for each alternative or for each risk profile. Because the outcomes occur statistically, an expected utility for the risk profile becomes a reasonable measure to unify the elementary utility values for outcomes in the profile.

The expected utility \( EU_1 \) for alternative \( A_1 \) is

\[
EU_1 = (0.3 \times U_{11}) + (0.7 \times U_{21}) \\
= (0.3 \times 1) + (0.7 \times 0.5) = 0.65
\]

while the expected utility \( EU_2 \) for alternative \( A_2 \) is

\[
EU_2 = (0.3 \times U_{12}) + (0.7 \times U_{22}) \\
= (0.3 \times 0) + (0.7 \times 1) = 0.7
\]

The second alternative, without the umbrella, is chosen because it has a larger expected utility. A person would take an umbrella, however, if elementary utility \( U_{21} \) is increased, for instance, to 0.9, which indicates that carrying the useless umbrella becomes a minor burden. A breakeven point for \( U_{21} \) satisfies \( 0.3 + 0.7U_{21} = 0.7 \), that is, \( U_{21} = (0.7 - 0.3)/0.7 = 0.57 \).

Sensitivity analyses similar to this can be performed for the likelihood of rain. Assume again the utility values in Table 1.2. Denote by \( P \) the probability of rain. Then, a breakeven point for \( P \) satisfies

\[
EU_1 = P \times 1 + (1 - P) \times 0.5 = P \times 0 + (1 - P) \times 1 = EU_2
\]

yielding \( P = 0.5 \). In other words, a person should not take the umbrella as long as the chance of rain is less than 50%.
The risk profile for each alternative now includes the utility $U_i$ (or significance):

$$\text{Risk} \equiv \{ (L_i, O_i, U_i) \mid i = 1, \ldots, n \} \quad (1.14)$$

This representation indicates an explicit dependence of a risk profile on outcome significance: the determination of the significance is a value judgment and is considered mainly in the risk-management phase. The significance is implicitly assumed when minor outcomes are screened out during the risk-assessment phase.

### 1.2.6 Causal Scenario

The likelihood as well as the outcome significance can be evaluated more easily when a causal scenario for the outcome is in place. Thus risk may be rewritten as

$$\text{Risk} \equiv \{ (L_i, O_i, U_i, C_{S_i}) \mid i = 1, \ldots, n \} \quad (1.15)$$

where $C_{S_i}$ denotes the causal scenario that specifies 1) causes of outcome $O_i$ and 2) event propagations for the outcome. This representation expresses an explicit dependence of risk profile on the causal scenario identified during the risk-assessment phase.

**Causal scenarios and PRA.** PRA uses, among other things, event tree and fault tree techniques to establish outcomes and causal scenarios. A scenario is called an accident sequence and is composed of various deleterious interactions among devices, software, information, material, power sources, humans, and environment. These techniques are also used to quantify outcome likelihoods during the risk-assessment phase.

**Example 4—Pressure tank PRA.** The system shown in Figure 1.9 discharges gas from a reservoir into a pressure tank [8]. The switch is normally closed and the pumping cycle is initiated by an operator who manually resets the timer. The timer contact closes and pumping starts.

![Figure 1.9. Schematic diagram of pressure tank system.](image-url)

Well before any over-pressure condition exists the timer times out and the timer contact opens. Current to the pump cuts off and pumping ceases (to prevent a tank rupture due to overpressure). If the
timer contact does not open, the operator is instructed to observe the pressure gauge and to open the manual switch, thus causing the pump to stop. Even if the timer and operator both fail, overpressure can be relieved by the relief valve.

After each cycle, the compressed gas is discharged by opening the valve and then closing it before the next cycle begins. At the end of the operating cycle, the operator is instructed to verify the operability of the pressure gauge by observing the decrease in the tank pressure as the discharge valve is opened. To simplify the analysis, we assume that the tank is depressurized before the cycle begins. An undesired event, from a risk viewpoint, is a pressure tank rupture due to overpressure.

Note that the pressure gauge may fail during the new cycle even if its operability was correctly checked by the operator at the end of the last cycle. The gauge can fail before a new cycle if the operator commits an inspection error.

Figure 1.10 shows the event tree and fault tree for the pressure tank rupture due to overpressure. The event tree starts with an initiating event that initiates the accident sequence. The tree describes combinations of success or failure of the system's mitigative features that lead to desired or undesired plant states. In Figure 1.10, $PO$ denotes the event "pump overrun," an initiating event that starts the potential accident scenarios. Symbol $OS$ denotes the failure of the operator shutdown system, $PP$ denotes failure of the pressure protection system by relief valve failure. The overbar indicates a logic complement of the inadvertent event, that is, successful activation of the mitigative feature. There are three sequences or scenarios displayed in Figure 1.10. The scenario labeled $PO \cdot OS \cdot PP$ causes overpressure and tank rupture, where symbol "•" denotes logic intersection, (AND). Therefore the tank rupture requires three simultaneous failures. The other two scenarios lead to safe results.

The event tree defines top events, each of which can be analyzed by a fault tree that develops more basic causes such as hardware or human faults. We see, for instance, that the pump overrun is caused by timer contact fails to open, or timer failure.* By linking the three fault trees (or their logic complements) along a scenario on the event tree, possible causes for each scenario can be enumerated. For instance, tank rupture occurs when the following three basic causes occur simultaneously: 1) timer contact fails to open, 2) switch contact fails to open, and 3) pressure relief valve fails to open. Probabilities for these three causes can be estimated from generic or plant-specific statistical data, and eventually the probability of the tank rupture due to overpressure can be quantified.

1.2.7 Population Affected

Final definition of risk. A population of a single individual is an exceptional case. Usually more than one person is affected anonymously by the risk. The population size is a factor that determines an important aspect of the risk. A comparison of risks using the Farmer curves in Figures 1.3 and 1.4 makes no sense unless the population is specified. The risk concept includes, as a final element, the population $PO_i$ affected by outcome $O_i$.

$$\text{Risk} \equiv \{ (L_i, O_i, U_i, CS_i, PO_i) \mid i = 1, \ldots, n \}$$  \hspace{1cm} (1.16)

Populations are identified during the risk-assessment phase.

1.2.8 Population Versus Individual Risk

Definitions of two types of risks. The term population risk is used when a population as a whole is at risk. A population risk is also called a societal risk, a collective risk, or a societally aggregated risk. When a particular individual in the population is the risk recipient, then the risk is an individual risk and the population $PO_i$ in the definition of risk reduces to a single person.

*Output event from an OR gate occurs when one or more input events occur; output event from an AND gate occurs when all input events occur simultaneously.
Figure 1.10. Event-tree and fault-tree analyses for pressure tank system.

Risk level measures. A risk profile is formally measured by an expected significance or utility (Table 1.5). A typical measure representing the level of individual risk is the likelihood or severity of a particular outcome or the expected outcome severity. Measures for the level of population risk are, for example, an expected number of people affected by the outcome or the sum of expected outcome severities.
If the outcome is a fatality, the individual risk level may be expressed by a fatal frequency (i.e., likelihood) per individual, and the population risk level by an expected number of fatalities. For radioactive exposure, the individual risk level may be measured by an individual dose (rem per person; expected outcome severity), and the population risk level by a collective dose (person rem; expected sum of outcome severities). The collective dose (or population dose) is the summation of individual doses over a population.

**Population-size effect.** Assume that a deleterious outcome brings an average individual risk of one fatality per million years, per person [9]. If 1000 people are affected by the outcome, the population risk would be $10^{-3}$ fatalities per year, per population. The same individual risk applied to the entire U.S. population of 235 million produces the risk of 235 fatalities per year. Therefore the same individual risk brings different societal risk depending on the size of the population (Figure 1.11).

![Population-size effect graph](image)

**Figure 1.11.** Expected number of annual fatalities under $10^{-6}$ individual risk.

Regulatory response (or no response) is likely to treat these two population risks comparably because the individual risk remains the same. However, there is a difference between the two population risks. There are severe objections to siting nuclear power plants within highly populated metropolitan centers; neither those opposed to nuclear power nor representatives from the nuclear power industry would seriously consider this option [3].

**Individual versus population approach.** An approach based on individual risk is appropriate in cases where a small number of individuals face relatively high risks; hence if the individual risk is reduced to a sufficiently small level, then the population risk also becomes sufficiently small. For a population of ten people, the population risk measured by
the expected number of fatalities is only ten times larger than the individual risk measured by fatality frequency. But when a large number of people faces a low-to-moderate risk, then the individual risk alone is not sufficient because the population risk might be a large number [9].

1.2.9 Summary

Risk is formally defined as a combination of five primitives: outcome, likelihood, significance, causal scenario, and population affected. These factors determine the risk profile. The risk-assessment phase deals with primitives other than the outcome significance, which is evaluated in the risk-management phase.

Each alternative for actively or passively controlling the risk creates a specific risk profile. The profile is evaluated using an expected utility to unify the outcome significance, and decisions are made accordingly. This point is illustrated by the min hazard mitigation problem. One-to-one correspondences exist among risk, risk profile, lottery, and alternative. A risk-free alternative is often used as a reference point in evaluating risky alternatives. Typical alternatives for risk control are listed in Table 1.3.

The pressure tank problem illustrates some aspects of probabilistic risk assessment. Here, the fault-tree technique is used in combination with the event-tree technique.

Two important types of risk are presented: individual risk and population risk. The size of the population is a crucial parameter in risk management.

1.3 SOURCE OF DEBATES

The previous section presents a rather simplistic view of risks and associated decisions. In practice, risk-assessment and -management viewpoints differ considerably from site to site. These differences are a major source of debate, and this section describes why such debates occur.

1.3.1 Different Viewpoints Toward Risk

Figure 1.12 shows perspectives toward risk by an individual affected, a population affected, the public, a company that owns and/or operates a facility, and a regulatory agency. Each has a different attitude toward risk assessment and management.

The elements of risk are likelihood, outcome, significance, causal scenario, and population. Risk assessment determines the likelihood, outcome, causal scenario, and population. Determination of significance involves a value judgment and belongs to the risk-management phase. An important final product of the management phase is a decision that requires more than outcome significances: the outcome significances must be synthesized into a measure that evaluates a risk profile containing plural outcomes (see Figure 1.8).

In the following sections, differences in risk assessment are described first by focusing on all risk elements except significance. Then the significance and related problems such as risk aversion are discussed in terms of risk management.

*The Nuclear Regulatory Commission recently reduced the distance for computing the population cancer fatality risk to 10 mi from 50 mi [10]. The average individual risk for the 10-mi distance is larger than the value for the 50-mi distance because the risk to people beyond 10 mi will be less than the risk to the people within 10 mi. Thus it makes sense to make regulations based on the conservative 10-mi individual risk. However, the 50-mi population risk could be significantly larger than the 10-mi population risk unless individual risk or population density diminish rapidly with distance.*
1.3.2 Differences in Risk Assessment

**Outcome and causal scenario.** Different people usually select different sets of outcomes because such sets are only obtainable through prediction. It is easy to miss novel outcomes such as, in the early 1980s, the transmission of AIDS by blood transfusion and sexual activity. Some question the basic premise of PRA—that is, the feasibility of enumerating all outcomes for new technologies and novel situations.

Event-tree and fault-tree techniques are used in PRA to enumerate outcomes and scenarios. However, each PRA creates different trees and consequently different outcomes and scenarios, because tree generation is an art, not a science. For instance, Figure 1.10 only analyzes tank rupture due to overpressure and neglects 1) a rupture of a defective tank under normal pressure, 2) an implosion due to low pressure, or 3) sabotage.

The nuclear power plant PRA analyzes core melt scenarios by event- and fault-tree techniques. However, these techniques are not the only ones used in the PRA. Containment capability after the core melt is evaluated by different techniques that model complicated physical and chemical dynamics occurring inside the containment and reactor vessels. Source terms (i.e., amount and types of radioactive materials released from the reactor site) from the containment are predicted as a result of such analyses. Different sets of assumptions and models yield different sets of scenarios and source terms.

**Population affected.** At intermediate steps of the PRA, only outcomes inside or on a boundary of the facility are dealt with. Examples of outcomes are chemical plant explosions, nuclear reactor core melts, or source terms. A technique called a consequence analysis is then performed to convert these internal or boundary outcomes into outside consequences such as radiation doses, property damage, and contamination of the environment. The consequence analysis is also based on uncertain assumptions and models. Figure 1.13 shows transport of the source term into the environment when a wind velocity is given.

**Outcome chain termination.** Outcomes engender new outcomes. The space shuttle schedule was delayed and the U.S. space market share reduced due to the Challenger accident. A manager of a chemical plant in Japan committed suicide after the explosion of his plant. Ultimately, outcome propagations terminate.

**Likelihood.** PRA uses event-tree and fault-tree techniques to search for basic causes of outcomes. It is assumed that these causes are so basic that historic statistical data are available to quantify the occurrence probabilities of these causes. This is feasible for simple hardware failures such as a pump failing to start and for simple human errors.
such as an operator inadvertently closing a valve. For novel hardware failures and for complicated cognitive human errors, however, available data are so sparse that subjective probabilities must be guesstimated from expert opinions. This causes discrepancies in likelihood estimates for basic causes.

Consider a misdiagnosis as the cognitive error. Figure 1.14 shows a schematic for a diagnostic task consisting of five activities: recollection of hypotheses (causes and their propagations) from symptoms, acceptance/rejection of a hypothesis in using qualitative or quantitative simulations, selection of a goal such as plant shutdown when the hypothesis is accepted, selection of means to achieve the goal, and execution of the means. A misdiagnosis occurs if an individual commits an error in any of these activities. Failure probabilities in the first four activities are difficult to quantify, and subjective estimates called expert opinions are often used.

Figure 1.13. Schematic description of source term transport.

Figure 1.14. Typical steps of diagnosis task.
The subjective likelihood is estimated differently depending on whether the risk is controlled by individuals or systems. Most drivers believe in their driving skills and underestimate likelihoods of their involvement in automobile accidents in spite of the fact that the statistical accident rate is derived from a population that largely includes the skilled drivers.

Quantification of basic causes must be synthesized into the outcome likelihood through AND and OR causal propagation logic. Again, event- and fault-tree techniques are used. There are various types of dependencies, however, among the basic and intermediate causes of the outcome. For instance, several valves may have been simultaneously left closed if the same maintenance person incorrectly manipulated them. Evaluation of this dependency is crucial in that it causes significant differences in outcome likelihood estimates.

By a nuclear PRA consequence analysis, the source term is converted into a radiation dose in units of rems or millirems (mrems) per person in a way partly illustrated in Figure 1.13. The individual or collective dose must be converted into a likelihood of cancers when latent fatality risk is quantified; a conservative estimate is a ratio of 135 fatalities per million person-rem. Figure 1.15 shows this conversion [11], where the horizontal and vertical axes denote amount of exposure in terms of person-rem and probability of cancer, respectively. A linear, nonthreshold, dose-rate-independent model is typical. Many radiologists, however, believe that this model yields an incorrect estimate of cancer probability. Some people use a linear-quadratic form, while others support a pure quadratic form.

![Figure 1.15. Individual dose and lifetime cancer probability.](image)

The likelihood may not be a unique number. Assume the likelihood is ambiguous and somewhere between 3 in 10 and 7 in 10. A likelihood of likelihoods (i.e., meta-likelihood) must be introduced to deal with the meta-uncertainty of the likelihood itself. Figure 1.4 included a meta-uncertainty as an error bound of outcome frequencies. People, however, may have different opinions about this meta-likelihood; for instance, any of 90%, 95%, or 99% confidence intervals of the likelihood itself could be used. Furthermore, some people challenge the feasibility of assigning likelihoods to future events; we may be completely ignorant of some likelihoods.
1.3.3 Differences in Risk Management

The risk profile must be evaluated before decision making begins. Such an evaluation first requires an evaluation of profile outcomes. As described earlier, outcomes are evaluated in terms of significance or utility. The outcome significances must be synthesized into a unified measure to evaluate the risk profile. In this way, each alternative and its risk profile is evaluated. In particular, people are strongly sensitive to catastrophic outcomes. This attitude toward risk is called risk aversion and manifests itself when we buy insurance. As will be discussed in Section 1.4, decision making under risk requires an understanding of this attitude.

This section first discusses outcome significances, available alternatives, and risk-profile significance. Then other factors such as outcome incommensurability, risk/cost trade-off, equity value concepts, and risk/cost/benefit trade-offs for decision making under risk are discussed. Finally, bounded rationality concepts and risk homeostasis are presented.

Loss or gain classification. Each outcome should be classified as a gain or loss. The PRA usually focuses on outcomes with obvious negativity (fatality, property damage). For other problems, however, the classification is not so obvious. People have their own reference point below which an outcome is regarded as a loss. Some references are objective and others are subjective. For investment problems, for instance, these references may be very complex.

Outcome significance. Each loss or gain must be evaluated by a significance or utility scale. Verbal and ambiguous measures such as catastrophic, severe, and minor may be used instead of quantitative measures. People have difficulty in evaluating the significance of an outcome never experienced: a habitual smoker can evaluate his lung cancer only postoperatively. The outcome significance depends on pairs of fuzzy antonyms: voluntary/involuntary, old/new, natural/man-made, random/nonrandom, accidental/intentional, forgettable/memorable, fair/unfair. Extreme categories (e.g., a controllable, voluntary, old outcome versus an uncontrollable, involuntary, new one) differ by many orders of magnitude on a scale of perceived risk [3]. The significance also depends on cultural attributes, ethics, emotion, reconciliation, media coverage, context, or litigability. People estimate the outcome significance differently when population risk is involved in addition to individual risk.

Available alternatives. Only one alternative is available for most people; the risk is uncontrollable, and they have to face it. Some people understand problems better and have more alternatives to reduce the risks. Gambles and business ventures are different fields of risk taking. In the former, risks are largely uncontrollable; in the latter, the risks are often controllable and avoidable. Obviously, different decisions are made depending on how many alternatives are available.

Risk-profile significance. Individuals may reach different decisions even if common sets of alternatives and associated risk profiles are given. Recall in the rain hazard mitigation problem in Section 1.2 that each significance is related to a particular outcome, not to a total risk profile. Because each alternative usually has two or more outcomes, these elementary significances must be integrated into a scalar by a suitable procedure, if the alternatives are to be arranged in a linear order. In the rain hazard mitigation problem an expected utility is used to unify significances of two outcomes for each alternative. In other words, a risk-profile significance of an alternative is measured by the expected utility. The
operation of taking an expected value is a procedure yielding the unified scalar significance. The alternative with a larger expected utility or a smaller expected significance is usually chosen.

**Expected utility.** The expected utility concept assumes that outcome significance can be evaluated independently of outcome likelihood. It also assumes that an impact of an outcome with a known significance decreases linearly with its occurrence probability when the outcome significance is given: [probability] × [significance]. The outcomes may be low likelihood–high loss (fatality), high likelihood–low loss (getting wet), or of intermediate severity. Some people claim that for the low-probability and high-loss events, the independence or the linearity in the expected utility is suspicious; one million fatalities with probability 10⁻⁶ may yield a more dreadful perception than one tenth of the perception of the same fatalities with probability 10⁻⁵. This correlation between outcome and likelihood yields different evaluation approaches for risk-profile significance for a given alternative.

**Incommensurability of outcomes.** It is difficult to combine outcome significances even if a single-outcome category such as fatalities or monetary loss is being dealt with. Unfortunately, loss categories are more diverse, for instance, financial, functional, time and opportunity, physical (plant, environmental damage), physiological (injury and fatality), societal, political. A variety of measures are available for approximating outcome significances: money, longevity, fatalities, pollutant concentration, individual and collective doses, and so on. Some are commensurable, others are incommensurable. Unification becomes far more difficult for incommensurable outcomes because of trade-offs.

**Risk/cost trade-off.** Even if the risk level is evaluated for each alternative, the decisions may not be easy. Each alternative has a cost.

**Example 5—Fatality goal and safety system expenditure.** Figure 1.16 is a schematic of a cost versus risk-profile trade-off problem. The horizontal and vertical axes denote the unified risk-profile significance in terms of expected number of fatalities and costs of alternatives, respectively. A population risk is considered. The costs are expenditures for safety systems. For simplicity of description, an infinite number of alternatives with different costs are considered. The feasible region of alternatives is the shaded area. The boundary curve is a set of equivalent solutions called a Pareto curve. The risk homeostasis line will be discussed later in this section. When two alternatives on the Pareto curve are given, we cannot say which one is superior. Additional information is required to arrange the Pareto alternatives in a linear preference order.

Assume that \( G_1 \) is specified as a maximum allowable goal of the expected number of fatalities. Then point \( A \) in Figure 1.16 is the most economical solution with cost \( C_1 \). The marginal cost at point \( A \) indicates the cost to decrease the expected number of fatalities by one unit, that is, cost to save a life. People have different goals, however; for the more demanding goal \( G_2 \), the solution is point \( B \) with higher cost \( C_2 \). The marginal cost generally tends to increase as the consequences diminish.

**Example 6—Monetary trade-off problem.** When fatalities are measured in terms of money, the trade-off problem is illustrated by Figure 1.17. Assume a situation where an outcome with ten fatalities occurs with frequency or probability \( P \) during the lifetime of a plant. The horizontal axis denotes the probability or frequency. The expected number of fatalities during the plant lifetime thus becomes 10 × \( P \). Suppose that one fatality cost \( A \) dollars. Then the expected lifetime cost \( C_0 \) potentially caused by the accident is 10 × \( A \times P \), which is denoted by the straight line passing through the origin. The improvement cost \( C_I \) for achieving the fatal outcome probability \( P \) is depicted by a hyperbolic-like curve where marginal cost increases for smaller outcome probabilities.

The total expected cost \( C_T = C_0 + C_I \) is represented by a unimodal curve with global minimal at \( TC \). As a consequence, the improvement cost at point \( IC \) is spent and the outcome probability
Figure 1.16. Trade-off problem between fatalities and reduction cost.

Figure 1.17. Trade-off problem when fatality is measured by monetary loss.

is determined. Point \(OC\) denotes the expected cost of the potential fatal outcome. The marginal improvement cost at point \(IC\) is equal to the slope \(10 \times A\) of the straight line \(O-OC\) of expected fatal outcome cost. In other words, the optimal slope for the improvement cost is determined as the cost of ten fatalities. Theoretically, the safety investment increases so long as the marginal cost with respect to outcome likelihood \(P\) is smaller than the cost of ten fatalities. Obviously, the optimal investment cost increases when either fatality cost \(A\) or outcome size (ten fatalities in this example) increases.

In actual situations, the plant may cause multiple outcomes with different numbers of fatalities. For such cases, a diagram similar to Figure 1.17 is obtained with the exception that the horizontal axis now denotes the number of expected fatalities from all plant scenarios. The optimal marginal improvement cost with respect to the number of expected fatalities (i.e., the marginal cost for decreasing one expected fatality) is equal to the cost of one fatality.
The cost versus risk-level trade-offs in Figures 1.16 and 1.17 make sense if and only if the system yields risk and benefits; if no benefit is perceived, the trade-off problem is moot.

**Equity value concept.** Difficult problems arise in quantifying life in terms of dollars, and an "equity value of saving lives" has been proposed rather than "putting a price on human life" [5]. According to the equity value theory, an alternative that leads to greater expenditures per life saved than numerous other alternatives for saving lives is an inequitable commitment of society's resources that otherwise could have been used to save a greater number of lives. We have to stop our efforts at a certain slope of the risk-cost diagram of Figure 1.16 for any system we investigate [12], even if our risk unit consists of fatalities. This slope is the price we can pay for saving a life, that is, the equity value.

This theory is persuasive if the resources are centrally controlled and can be allocated for any purpose whatsoever. The theory becomes untenable when the resources are privately or separately owned: a utility company would not spend their money to improve automobile safety; people in advanced countries spend money to save people from heart diseases, while they spend far less money to save people from starvation in Africa.

**Risk/cost/benefit (RCB) trade-off.** According to Starr [13],

the electricity generation options of coal, nuclear power, and hydroelectricity have been compared as to benefits and risks, and been persuasively defended by their proponents. In retrospect, the past decade has shown that the comparative risk perspective provided by such quantitative analysis has not been an important component of the past decisions to build any of these plants. Historically, initial choices have been made on the basis of performance economics and political feasibility, even in the nuclear power program.

Many technologies start with emphases on their positive aspects—their merits or benefits. After a while, possibly after a serious accident, people suddenly face the problem of choosing one of two alternatives, that is, accepting or rejecting the technology. Ideally, but not always, they are shown a risk profile of the alternative together with the benefits from the technology. Decision making of this type occurs daily at hospitals before or during a surgical operation; the risk profile there would be a Farmer curve with the horizontal axis denoting longevity loss or gain, while the vertical axis is an excess probability per operation.

Figure 1.18 shows another schematic relation between benefit and risk. The higher the benefit, the higher the risk. A typical example is a heart transplant versus an anticlotting drug.

![Figure 1.18. Schematic relation between benefits and acceptable risks.](image-url)
**Bounded rationality concept.** Traditional decision-making theory makes four assumptions about decision makers.

1. They have a clearly defined utility value for each outcome.
2. They possess a clear and exhaustive view of the possible alternatives open to them.
3. They can create a risk profile for the future associated with each alternative.
4. They will choose between alternatives to maximize their expected utility.

However, flesh and blood decision making falls short of these Platonian assumptions. In short, human decision making is severely constrained by its keyhole view of the problem space that is called “bounded rationality” by Simon [14]:

The capacity of the human mind for formulating and solving complex problems is very small compared with the size of the problems whose solutions are required for objectively rational behavior in the real world—or even for a reasonable approximation of such objective rationality.

The fundamental limitation in human information processing gives rise to “satisficing” behavior, that is, the tendency to settle for satisfactory rather than optimal courses of action.

**Risk homeostasis.** According to risk homeostasis theory [15], the solution with cost $C_2$ in Figure 1.16 tends to move to point $H$ as soon as a decision maker changes the goal from $G_1$ to $G_2$: the former risk level $G_1$ is thus revisited. The theory states that people have tendencies to keep a constant risk level even if a safer solution is available. When a curved freeway is straightened to prevent traffic accidents, drivers tend to increase their speed, and thus incur the same risk level as before.

1.3.4 **Summary**

Different viewpoints toward risk are held by the individual affected, the population affected, the public, companies, and regulatory agencies. Disagreements arising in the risk-assessment phase encompass outcome, causal scenario, population affected, and likelihood, while in the risk-management phase disagreement exists in loss/gain classification, outcome significance, available alternatives, risk profile significances, risk/cost trade-off, and risk/cost/benefit trade-off.

The following factors make risk management difficult: 1) incommensurability of outcomes, 2) bounded rationality, and 3) risk homeostasis. An equity value guideline is proposed to give insight for the trade-off problem between monetary value and life.

### 1.4 Risk-Aversion Mechanisms

PRAM involves both objective and subjective aspects. A typical subjective aspect arising in the risk-management phase is an instinctive attitude called risk aversion, which is introduced qualitatively in Section 1.4.1. Section 1.4.2 describes three attitudes toward monetary outcomes: risk aversion, risk seeking, and risk neutral. Section 1.4.3 shows that the monetary approach can fail in the face of fatalities. Section 1.4.4 deals with an explanation of postaccident overestimation of outcome severity and likelihood. Consistent Bayesian explanations are given in Sections 1.4.5 and 1.4.6 with emphasis on a posteriori distribution. A public confidence problem with respect to the PRAM methodology is described in Section 1.4.7.
1.4.1 Risk Aversion

It is believed that people have an ambivalent attitude toward catastrophic outcomes; small stimuli distributed over time or space are ignored, while the sum of these stimuli, if exerted instantly and locally, cause a significant response. For instance, newspapers ignore ten single-fatality accidents but not one accident with ten fatalities. In order to avoid worst-case potential scenarios, people or companies buy insurances and pay amounts that are larger than the expected monetary loss. This attitude is called risk aversion.

One reason for the dispute about nuclear power lies in attitude toward risk. In spite of the high population risk, people pay less attention to automobile accidents, which cause more than ten thousand fatalities every year, because these accidents occur in an incremental and dispersed manner; however, people react strongly to a commercial airline accident where several hundred people die simultaneously. In addition to the individual- versus population-risk argument, the risk-aversive attitude is an unavoidable subject in the risk-management field.

1.4.2 Three Attitudes Toward Monetary Outcome

Risk-aversive, neutral, and seeking. People perceive the significance of money differently; its significance or utility is not necessarily proportional to the amount. Figure 1.19 shows three attitudes in terms of loss or value function curves: risk-aversive (convex), risk-seeking (concave), and risk-neutral (linear). For the loss function curves, the positive direction of the horizontal axis denotes more loss, and the negative direction more gain; the vertical axis denotes the loss significance of money. Each point on the monotonously increasing loss significance curve \( O-B-C-L \) in the upper-left-corner graph denotes a significance value for each insurance premium dollar spent, that is, a loss without uncertainty. The smaller the significance value, the lower the loss. Each point on the third quadrant curve, which is also monotonously increasing, denotes a significance value for a dollar gain.

Convex significance curve. A convex curve \( s(x) \) is defined mathematically by the inequality holding for all \( x \), \( x_2 \), and probability \( P \).

\[
s[Px_2 + (1 - P)x_1] \leq Ps(x_2) + (1 - P)s(x_1)
\]  

(1.17)

Insurance premium loss versus expected loss. Figure 1.20 shows an example of a convex significance curve \( s(x) \). Consider the risk scenario as a lottery where \( x_1 \) and \( x_2 \) amounts of money are lost with probability \( 1 - P \) and \( P \), respectively. As summarized in Table 1.6, the function on the left-hand side of the convex curve definition denotes the significance of the insurance premium \( Px_2 + (1 - P)x_1 \). This premium is equal to the expected amount of monetary loss from the lottery. Term \( Ps(x_2) + (1 - P)s(x_1) \) on the right-hand side is the expected significance when two significances \( s(x_1) \) and \( s(x_2) \) for loss \( x_1 \) and \( x_2 \) occur with the same probabilities as in the lottery; thus the right-hand side denotes a significance value of the lottery itself. The convexity implies that the insurance premium loss is preferred to the lottery.

Avoidance of worse case. Because the insurance premium \( Px_2 + (1 - P)x_1 \) is equal to the expected loss of the lottery, one of the losses (say \( x_2 \)) is greater than the premium loss, indicating that the risk-averse attitude avoids the worse case \( x_2 \) in the lottery; in other words, risk-averse people will pay the insurance premium to compensate for the potentially
worse-loss outcome $x_2$. A concave curve for the risk-seeking attitude is defined by a similar inequality, but the inequality sign is reversed.

**Example 7—A lottery and premium-paid.** Point $A$ in the upper-left-corner graph of Figure 1.19 is the middle point of a straight line segment between points $O$ and $L$. The vertical coordinate of this point indicates a loss significance value of a lottery where getting $1000 or nothing occurs with equal probabilities $P = 0.5$, respectively; the lottery is evaluated according to the expected significance, $0.5 \times s(0) + 0.5 \times s(1000) = s(1000)/2$. The horizontal coordinate of point $A$ is a $500 premium, which is equal to the expected loss of the lottery. Because the curve is convex, the line segment $O-L$ is always above the nonlinear curve and we see that the premium loss of $500 is preferred to the lottery with the same expected loss of money.

**Example 8—Insurance premium and lottery range.** Point $C$ indicates an insurance payment with equivalent loss significance to the lottery denoted by point $A$. Thus the lottery can be
TABLE 1.6. Insurance Premium Significance and Expected Lottery Significance

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P$</td>
<td>Probability of loss $x_2$</td>
</tr>
<tr>
<td>$1 - P$</td>
<td>Probability of loss $x_1$</td>
</tr>
<tr>
<td>$Px_2 + (1 - P)x_1$</td>
<td>Expected lottery loss</td>
</tr>
<tr>
<td>$Px_2 + (1 - P)x_1$</td>
<td>Insurance premium</td>
</tr>
<tr>
<td>$s(Px_2 + (1 - P)x_1)$</td>
<td>Insurance premium significance</td>
</tr>
<tr>
<td>$Ps(x_2) + (1 - P)s(x_1)$</td>
<td>Expected lottery significance</td>
</tr>
</tbody>
</table>

The significance curve is convex for the risk-aversive attitude and the marginal loss significance increases with the amount of lost money. According to the attitude, the $1000 premium paid by a particular person is more serious than the $100 premiums distributed among and paid by ten persons, provided that these persons have the same risk-aversion attitude. This is analogous to viewing a ten-fatality accident involving a single automobile as more serious than one-fatality accidents distributed over ten automobiles.
Risk-seeking and -neutral. For the risk-seeking attitude in the lower-left-corner graph of Figure 1.19, the straight line segment is below the nonlinear concave significance curve, and the fifty-fifty lottery is preferred to the premium loss of $500; the marginal significance decreases with the amount of lost money. The upper-right-corner graph shows a risk-neutral attitude, where a lottery with an expected loss of $500 is not distinguishable from the $500 premium loss. The marginal significance remains constant.

Utility of monetary outcome. When the horizontal and vertical axes are reversed, curves in terms of utility appear. The lower-right-corner graph of Figure 1.19 shows risk-aversive, risk-seeking, and risk-neutral utility curves that are concave, convex, and linear, respectively. The risk-aversion is represented by convex and concave curves for significance and utility, respectively. For the risk-aversive curve, marginal utility decreases with the increase of certain gain or the decrease of certain loss.

1.4.3 Significance of Fatality Outcome

When fatalities are involved, the previous risk-aversion and -seeking lottery problem described in terms of monetary outcomes becomes much more complicated. Figure 1.21 shows a case where one sure fatality is compared with a lottery that causes two and zero fatalities with equal probability 0.5. The expected number of fatalities in the lottery is just one. If a mother with two children is risk averse, as is usually assumed, then she should choose certain death of one child to avoid the more serious potential death of two children. The choice is reversed if the mother is risk seeking.

The risk-seeking behavior is the intuitive outcome because, among other things, the sacrifice of one child is not justified ethically, emotionally, or rationally. However, this comparison of a certain death with potential deaths is totally sophomoric because only a sadist would pose such a question, and only a masochist would answer it. Another viewpoint is that the fatality has an infinite significance value, and we cannot compare one infinity with another when a sure fatality is involved.

Figure 1.21. Comparison of one sure fatality with 50% chance of two fatalities.
1.4.4 Mechanisms for Risk Aversion

Overestimation of frequency and outcome. A more reasonable explanation of risk aversiveness for outcomes including fatalities was given by Bohnenblust and Schneider in Switzerland [12]. According to them, misestimations of risks after severe accidents are one of the major reasons for risk-aversive attitudes, which prefer ten single-fatality accidents to one accident with ten fatalities. Risks can be misestimated or overestimated with respect to size or likelihood of outcomes. This is similar to the error bands depicted in Figure 1.4, where the uncertainty is either due to errors of frequency or outcome severity estimation.

Overestimating outcome severity. Consider first the misestimation of an outcome severity such as the number of fatalities. Imagine a system that causes, on the average, one accident every one hundred years. Most of these accidents have relatively small consequences, say one fatality for each. Once in a while there may be a catastrophic event with ten fatalities. If the catastrophic event happens to occur, the public (or regulatory agencies) may believe that all accidents have catastrophic outcomes, thus they demand more safety measures than are justified by the actual damage expectation. Such a claim is not restricted to the particular facility that caused the accident; improvements are required for all other facilities of this type. As a consequence, all operators of this type of facility must adopt a risk-averse behavior to avoid the excessive consequences caused by the one large accident.

Overestimation of outcome likelihood. Suppose that at a plant there is a one chance in ten thousand years for a serious accident. After the occurrence of such an accident, however, the public perception is no longer that the installation has an accident interval of ten thousand years. The public might force the company to behave as if an accident occurred every thousand years, not every ten thousand years. This means that the risk and therefore the safety costs are overestimated by a factor of ten.

Erosion of public confidence. In the “Policy Statement on Safety Goals for the Operation of Nuclear Power Plants” published on August 4, 1986, the U.S. Nuclear Regulatory Commission (NRC) recognizes that, apart from their health and safety consequences, severe core damage accidents can erode public confidence in the safety of nuclear power and can lead to further instability and unpredictability for the industry. In order to avoid these adverse consequences, the Commission intends to continue to pursue a regulatory program with an objective of providing reasonable assurance, while giving appropriate consideration to the uncertainties involved [10].

1.4.5 Bayesian Explanation of Severity Overestimation

A priori distribution of defects. The public’s and regulatory agencies’ overestimation may not be a misestimation; it is consistent with a result from Bayesian statistics.* Assume that the accident occurs at a rate of once in one hundred years. Suppose that there is a debate about whether or not this type of facility poses a serious safety problem. The public believes a priori that the existence and nonexistence of the defect are equally probable, that is, $P = 0.5$; if the defect exists, the accident yields 10 fatalities with probability 0.99, and 1 fatality with probability 0.01; if the defect does not exist, these probabilities are reversed.

*The appendix of Chapter 3 describes the Bayes theorem for readers unfamiliar with Bayesian statistics.
A posteriori distribution of defects. Consider how the public belief about the defect changes when the first accident yields ten fatalities. According to the Bayes theorem, we have a posteriori probability of a defect conditioned by the occurrence of the ten-fatality accident.

\[
\Pr\{\text{Defect} \mid 10\} = \frac{\Pr\{\text{Defect}, 10\}/\Pr\{10\}}{\Pr\{\text{Defect}\Pr\{10 \mid \text{Defect}\} + \Pr\{\text{No defect}\Pr\{10 \mid \text{No defect}\}\}} = 0.5 \times 0.99 \quad (1.18)
\]

Even if the first accident was simply bad luck, the public does not think that way; public belief is that in this type of facility the probability of a serious defect increases to 0.99 from 0.5, yielding the belief that future accidents are almost certain to cause ten fatalities. An example is the Chernobyl nuclear accident. Experts alleviated the public postaccident shock by stating that the Chernobyl graphite reactor had a substantial defect that U.S. reactors do not have.

Gaps between experts and public. It can be argued that the public a priori distribution

\[
\Pr\{\text{Defect}\} = \Pr\{\text{No defect}\} = 0.5 \quad (1.21)
\]

is questionable in view of the PRA that gives a far smaller a priori defect probability. However, such a claim will not be persuasive to the public that has little understanding of the PRA, and who places more emphasis on the a posteriori information after the real accident, than on the a priori calculation before the accident. Spangler summarizes gaps in the treatment of technological risks by technical experts and the lay public, as given in Tables 1.7 and 1.8 [5,16].

1.4.6 Bayesian Explanation of Likelihood Overestimation

A priori frequency distribution. The likelihood overestimation can also be explained by a Bayesian approach. Denote by \( F \) the frequency of the serious accident. Before the accident the public accepted the following a priori distribution of the frequency: \( \Pr\{F = 10^{-4}\} = 0.99 \) and \( \Pr\{F = 10^{-2}\} = 0.01 \).

A posteriori distribution of frequency. Assume the first serious accident occurred after one year’s operation of the facility. Then the a posteriori distribution of the frequency after accident \( A \) is

\[
\Pr\{F = 10^{-2} \mid A\} = \frac{\Pr\{F = 10^{-2}, A\}/\Pr\{A\}}{\Pr\{F = 10^{-2}\Pr\{A \mid F = 10^{-2}\} \} = 0.01 \times 0.01 \quad (1.22)
\]

An accident per one hundred years now becomes as plausible as an accident per ten thousand years. The public will not think that the first accident was simply bad luck.
TABLE 1.7. Treatment of Technological Risks by Technical Experts

<table>
<thead>
<tr>
<th>Approach</th>
<th>Treatment Common to Experts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Criteria for risk acceptance</td>
<td>Risk judged in both absolute and relative terms</td>
</tr>
<tr>
<td>a. Absolute vs relative risk</td>
<td>Essential to sound decision making because of finite societal resources for risk reduction and impracticability of achieving zero risk; tends to ignore nondollar costs in such trade-offs</td>
</tr>
<tr>
<td>b. Risk-cost trade-offs</td>
<td>Emphasizes total (net) benefits to society, neglecting benefits that are difficult to quantify; also neglects indirect and certain long-term benefits</td>
</tr>
<tr>
<td>c. Risk-benefit comparisons of technological options</td>
<td>Tends to treat shallowly without explicit decision criteria and structured analyses</td>
</tr>
<tr>
<td>d. Equity consideration</td>
<td></td>
</tr>
<tr>
<td>2. Risk-assessment methods</td>
<td>Quantitative</td>
</tr>
<tr>
<td>a. Expression mode</td>
<td>Computational</td>
</tr>
<tr>
<td>b. Logic mode</td>
<td>• Risk = consequence × probability</td>
</tr>
<tr>
<td></td>
<td>• Fault trees/event trees</td>
</tr>
<tr>
<td></td>
<td>• Statistical calculation</td>
</tr>
<tr>
<td>c. Learning mode</td>
<td>Experimental</td>
</tr>
<tr>
<td></td>
<td>• Laboratory animals</td>
</tr>
<tr>
<td></td>
<td>• Clinical data for humans</td>
</tr>
<tr>
<td></td>
<td>• Engineering test equipment and simulators</td>
</tr>
<tr>
<td>3. Basis for trusting information</td>
<td>Established institutions</td>
</tr>
<tr>
<td>a. Source preference</td>
<td>Qualification of experts</td>
</tr>
<tr>
<td>b. Source reliability</td>
<td>Robustness/uncertainty of scientific knowledge</td>
</tr>
<tr>
<td>c. Accuracy of information</td>
<td></td>
</tr>
<tr>
<td>4. Risk-attribute evaluation</td>
<td>Objective, conservative assessment</td>
</tr>
<tr>
<td>a. Low-frequency risk</td>
<td>Broad range of high and low estimates</td>
</tr>
<tr>
<td>b. Newness of risk</td>
<td>Gives equal weight</td>
</tr>
<tr>
<td>c. Catastrophic vs dispersed deaths</td>
<td>Diverse views over treatment of incommensurables and discount rate</td>
</tr>
<tr>
<td>d. Immediate vs delayed deaths</td>
<td>Gives equal weight</td>
</tr>
<tr>
<td>e. Statistical vs known deaths</td>
<td>Generally ignores</td>
</tr>
<tr>
<td>f. Dreadfulness of risk</td>
<td>Gives equal weight</td>
</tr>
<tr>
<td>g. Voluntary vs involuntary risk</td>
<td></td>
</tr>
<tr>
<td>5. Technological consideration</td>
<td>Stimulus for redundancy and defense-in-depth in system design and operating procedures; margins of conservatism in design; quality assurance programs</td>
</tr>
<tr>
<td>a. Murphy’s law (if anything can go wrong, it will)</td>
<td>Valued source of data for technological fixes and prioritizing research; increased attention to consequence mitigation</td>
</tr>
</tbody>
</table>
### TABLE 1.8. Treatment of Technological Risks by Lay Public

<table>
<thead>
<tr>
<th>Approach</th>
<th>Treatment Common to the Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Criteria for risk acceptance</td>
<td></td>
</tr>
<tr>
<td>a. Absolute vs relative risk</td>
<td>Greater tendency to judge risk in absolute terms</td>
</tr>
<tr>
<td>b. Risk-cost trade-offs</td>
<td>Because human life is priceless, criteria involving risk-cost trade-offs are immoral; ignores</td>
</tr>
<tr>
<td></td>
<td>risks of no-action alternatives to rejected technology; gives greater weight to nondollar costs</td>
</tr>
<tr>
<td>c. Risk-benefit comparisons of technological options</td>
<td>Emphasizes personal rather than societal benefits; includes both qualitative and quantitative</td>
</tr>
<tr>
<td></td>
<td>benefits but tends to neglect indirect and long-term benefits</td>
</tr>
<tr>
<td>d. Equity consideration</td>
<td>Tends to distort equity considerations in favor of personal interests to the neglect of the</td>
</tr>
<tr>
<td></td>
<td>interests of opposing parties or the common good of society</td>
</tr>
<tr>
<td>2. Risk-assessment methods</td>
<td>Qualitative</td>
</tr>
<tr>
<td>a. Expression mode</td>
<td>Intuitive</td>
</tr>
<tr>
<td>b. Logic mode</td>
<td>• Incomplete rationale</td>
</tr>
<tr>
<td></td>
<td>• Emotional input to value judgments</td>
</tr>
<tr>
<td>c. Learning mode</td>
<td>Impressionistic</td>
</tr>
<tr>
<td></td>
<td>• Personal experience/memory</td>
</tr>
<tr>
<td></td>
<td>• Media accounts</td>
</tr>
<tr>
<td></td>
<td>• Cultural exchange</td>
</tr>
<tr>
<td>3. Basis for trusting information</td>
<td>Nonestablishment sources</td>
</tr>
<tr>
<td>a. Source preference</td>
<td>Limited ability to judge qualifications</td>
</tr>
<tr>
<td>b. Source reliability</td>
<td>Minimal understanding of strengths and limitations of scientific knowledge</td>
</tr>
<tr>
<td>c. Accuracy of information</td>
<td></td>
</tr>
<tr>
<td>4. Risk-attribute evaluation</td>
<td></td>
</tr>
<tr>
<td>a. Low-frequency risk</td>
<td>Tends to exaggerate or ignore risk</td>
</tr>
<tr>
<td>b. Newness of risk</td>
<td>Tends to exaggerate or ignore risk</td>
</tr>
<tr>
<td>c. Catastrophic vs dispersed deaths</td>
<td>Gives greater weight to catastrophic deaths</td>
</tr>
<tr>
<td>d. Immediate vs delayed deaths</td>
<td>Gives greater weight to immediate deaths except for known exposure to cancer-producing agents</td>
</tr>
<tr>
<td>e. Statistical vs known deaths</td>
<td>Gives greater weight to known deaths</td>
</tr>
<tr>
<td>f. Dreadfulness of risk</td>
<td>Gives greater weight to dreaded risk</td>
</tr>
<tr>
<td>g. Voluntary vs involuntary risk</td>
<td>Gives greater weight to involuntary risk</td>
</tr>
<tr>
<td>5. Technological consideration</td>
<td></td>
</tr>
<tr>
<td>a. Murphy’s law (if anything can go wrong, it will)</td>
<td>Stimulus for what-if syndromes and distrust of technologies and technocrats; source of</td>
</tr>
<tr>
<td></td>
<td>exaggerated views on risk levels using worst-case assumptions</td>
</tr>
<tr>
<td>b. Reports of technological failures and accidents</td>
<td>Confirms validity of Murphy’s law; increased distrust of technocrats</td>
</tr>
</tbody>
</table>
1.4.7 PRAM Credibility Problem

In Japan some people believe that the engineering approaches such as PRA are relatively useless for gaining public acceptance of risky facilities. Perhaps credibilities gained by sharing a bottle of wine are more crucial to human relations. Clearly, the PRAM methodology requires more psychosocial research to gain public credit.

According to Chauncey Starr of the Electric Power Research Institute [13]:

Science cannot prove safety, only the degree of existing harm. In the nuclear field emphasis on PRA has focused professional concern on the frequency of core melts. The arguments as to whether a core can melt with a projected probability of one in a thousand per year, or in a million per year, represent a misplaced emphasis on these quantitative outcomes. The virtue of the risk assessments is the disclosure of the system's causal relationships and feedback mechanisms, which might lead to technical improvements in the performance and reliability of the nuclear stations. When the probability of extreme events becomes as small as these analyses indicate, the practical operating issue is the ability to manage and stop the long sequence of events which could lead to extreme end results. Public acceptance of any risk is more dependent on public confidence in risk management than on the quantitative estimates of risk consequences, probabilities and magnitudes.

1.4.8 Summary

Risk aversion is defined as the subjective attitude that prefers a fixed loss to a lottery with the same amount of expected loss. When applied to monetary loss, risk aversion implies convex significance curves, monotonously increasing marginal significance, and insurance premiums larger than the expected loss. A risk-seeking or risk-neutral attitude can be defined in similar ways. The comparison approach between the fixed loss and expected loss, however, cannot apply to fatality losses.

Postaccident overestimation in outcome severity or in outcome frequency can be explained by the Bayes theorem. The public places more emphasis on the a posteriori distribution after an accident than on the a priori PRA calculation.

1.5 SAFETY GOALS

When goals are given, risk problems become more tractable; risk management tries to satisfy the goals, and the risk assessment checks the attainment of the goals. Goals for risk management can be specified in terms of various measures including availability, reliability, risk, and safety. Aspects of these measures are clarified in Section 1.5.1. A hierarchical arrangement of the goals is given in Section 1.5.2. Section 1.5.3 shows a three-layer decision structure with upper and lower bound goals. Examples of goals are given in Sections 1.5.4 and 1.5.5 for normal activities and catastrophic accidents, respectively. Differences between idealistic and pragmatic lower bound goals are described in Section 1.5.6, where the concept of regulatory cutoff level is introduced. The final section gives a model for varying the regulatory cutoff level as a function of population size.

1.5.1 Availability, Reliability, Risk, and Safety

Availability is defined as the characteristic of an item expressed by the probability that it will be operational at a future instant in time (IEEE Standard 352). In this context, a protection device such as a relief valve is designed to exhibit a high availability.
Reliability is defined as a probability that an item will perform a required function when used for its intended purpose, under the stated conditions, for a given period of time [4]. The availability is measured at an instant, and the reliability during a period of time.

Availability and reliability are independent of who is causing the loss outcome and who is exposed to it. On the other hand, risk depends on the gain/loss assignment of the outcome to people involved; shooting escaping soldiers is a gain for the guards, while being shot is a loss for the escapees. Safety is only applicable to the people subject to the potential loss outcome. That is, safety is originally a concept viewed from the aspect of people who are exposed to the potential loss.

Fortunately, this subtle difference among availability, reliability, risk, and safety is usually irrelevant to PRAM where the people involved are supposed to be honest enough to try to decrease potential losses to others. An alternative with less risk is thus considered safer; an instrument with a high availability or reliability is supposed to increase safety. Safety can thus be regarded as inversely proportional to the risk, and both terms are used interchangeably; it is, however, also possible for a company spending too much for safety to face another risk: bankruptcy.

1.5.2 Hierarchical Goals for PRAM

Systems subject to PRA have a hierarchical structure: components, units, subsystems, plant, and site. Safety goals also form a hierarchy. For a nuclear power plant, for instance, goals can be structured in the following way [17] (see Figure 1.22):

1. Initiating event level: occurrence frequency
2. Safety system level: unavailability
3. Containment: failure probability
4. Accident sequence level: sequence frequency
5. Plant: damage frequency, source term
6. Site and environment: collective dose, early fatalities, latent cancer fatalities, property damage

The safety goals at the top of the hierarchy are most important. For the nuclear power plant, the top goals are those on the site and environment level. When the goals on the top level are given, goals on the lower levels can, in theory, be specified in an objective and systematic way. If a hierarchical goal system is established in advance, the PRAM process is simplified significantly: the probabilistic risk-assessment phase, given alternatives, calculates performance indices for the goals on various levels, with error bands. The risk-management phase proposes the alternatives and evaluates the attainment of the goals.

To achieve goals on the various levels, a variety of techniques are proposed: suitable redundancy, reasonable isolation, sufficient diversity, sufficient independence, and sufficient margin [17]. Appendix A to Title 10 of the Code of Federal Regulations Part 50 (CFR Part 50) sets out 64 general design criteria for quality assurance: protection against fire, missiles, and natural phenomena; limitations on the sharing of systems; and other protective safety requirements. In addition to the NRC regulations, there are numerous supporting guidelines that contribute importantly to the achievement of safety goals. These include regulatory guides (numbering in the hundreds); the Standard Review Plan for reactor license applications, NUREG-75/087 (17 chapters); and associated technical positions and appendices in the Standard Review Plan [10].
1.5 Safety Goals

Site and Environment
- Early Fatalities
- Latent Fatalities
- Property Damage
- Population Exposure

Plant
- Damage Frequency
- Released Material

Accident Sequence
- Frequency

Initiating Event
- Frequency

Safety System
- Unavailability

Containment Barrier
- Failure Probability

Figure 1.22. Hierarchy of safety goals.

1.5.3 Upper and Lower Bound Goals

Three-layer decision structure. Cyril Comar [18] proposed the following decision structure, as cited by Spangler [5]:

1. Eliminate any risk that carries no benefit or is easily avoided.
2. Eliminate any large risk \( U \) that does not carry clearly overriding benefits.
3. Ignore for the time being any small risk \( L \) that does not fall into category 1.
4. Actively study risks falling between these limits, with the view that the risk of taking any proposed action should be weighed against the risk of not taking that action.

Of course, upper bound level \( U \) is greater than lower bound level \( L \). The shaded areas in Figure 1.23 show acceptable risk regions with an elimination level \( L \). The easily avoided risk in the first statement can, by definition, be reduced below \( L \) regardless of the merits. The term risk is used mainly to denote a risk level in terms of outcome likelihood. The term action in the fourth statement means an alternative; thus action is not identical to a risk source such as a nuclear power plant or chemical plant; elimination of a particular action does not necessarily imply elimination of the risk source; the risk source may continue to exist when other actions or alternatives are introduced.

In Comar's second statement, the large risk \( U \) is reluctantly accepted if and only if it has overriding benefits such as risks incurred by soldiers at war (national security) or patients undergoing operations (rescue from a serious disease). Denote by \( R \) the risk level of an action. Then the decision structure described above can be as stated in Figure 1.24.

We see that only risks with moderate benefits are subject to the main decision structure, which consists of three layers separated by upper and lower limits \( U \) and \( L \), respectively: \( R \geq U, L < R < U, \) and \( R \leq L \). In the top layer \( R \geq U \), the risk is first reduced below \( U \);
Figure 1.23. Three-layer decision structure.

Figure 1.24. Algorithm for three-layer decision structure.

the resultant level may locate in the middle $L < R < U$ or the bottom layer $R \leq L$. In the middle layer, risk $R$ is actively studied by risk-cost-benefit (RCB) analyses for justification; if it is justified, then it is reluctantly accepted; if it is not justified, then it is reduced until justification in the middle layer or inclusion in the bottom layer. In the bottom layer, the risk is automatically accepted even if it carries no benefits.

Note that the term *reduce* does not necessarily mean an immediate reduction; rather it denotes registration into a reduction list; some risks in the top layer or some risks not
justified in the middle layer are difficult to reduce immediately but can be reduced in the future; some other risks such as background radiation, which carries no benefits, are extremely difficult to reduce in the prescreening structure, and would remain in the reduction list forever.

The lower bound $L$ is closely related to the de minimis risk (to be described shortly), and its inclusion can be justified for the following reasons: 1) people do not pay much attention to risks below the lower bound even if they receive no benefits, 2) it becomes extremely difficult to decrease the risk below the lower bound, 3) there are almost countless and hence intractable risks below the lower bound, 4) above the lower bound there are many risks in need of reduction, and 5) without such a lower bound, all company profits could be allocated for safety [19].

**Upper and lower bound goals.** Comar defined the upper and lower bounds by probabilities of fatality of an individual per year of exposure to the risk.

$$U = 10^{-4}/\text{(year, individual)}, \quad L = 10^{-5}/\text{(year, individual)}$$ (1.25)

Wilson [20] defined the bounds for the individual fatal risk as follows.

$$U = 10^{-3}/\text{(year, individual)}, \quad L = 10^{-6}/\text{(year, individual)}$$ (1.26)

According to annual statistical data per individual, “being struck by lightning” is smaller than $10^{-6}$, “natural disasters” stands between $10^{-6}$ and $10^{-5}$, “industrial work” is between $10^{-5}$ and $10^{-4}$, and “traffic accidents” and “all accidents” fall between $10^{-4}$ and $10^{-3}$ (see Table 1.9).

**TABLE 1.9. Order of Individual Annual Likelihood of Early Fatality**

<table>
<thead>
<tr>
<th>Annual Likelihood</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^{-4}$ to $10^{-3}$</td>
<td>All accidents</td>
</tr>
<tr>
<td>$10^{-4}$ to $10^{-3}$</td>
<td>Traffic accidents</td>
</tr>
<tr>
<td>$10^{-5}$ to $10^{-4}$</td>
<td>Industrial work</td>
</tr>
<tr>
<td>$10^{-5}$</td>
<td>Drowning</td>
</tr>
<tr>
<td>$10^{-5}$</td>
<td>Air travel</td>
</tr>
<tr>
<td>$10^{-5}$</td>
<td>Drinking five liters of wine</td>
</tr>
<tr>
<td>$10^{-6}$ to $10^{-5}$</td>
<td>Natural disasters</td>
</tr>
<tr>
<td>$10^{-6}$</td>
<td>Smoking three U.S. cigarettes</td>
</tr>
<tr>
<td>$10^{-6}$</td>
<td>Drinking a half liter of wine</td>
</tr>
<tr>
<td>$10^{-6}$</td>
<td>Visiting New York or Boston for two days</td>
</tr>
<tr>
<td>$10^{-6}$</td>
<td>Spending six minutes in canoe</td>
</tr>
<tr>
<td>$&lt; 10^{-7}$</td>
<td>Lightning, tornadoes, hurricanes</td>
</tr>
</tbody>
</table>

Because the upper bound suggested by Comar is $U = 10^{-4}$, the current traffic accident risk level $R \geq U$ would imply the following: automobiles have overriding merits and are reluctantly accepted in the prescreening structure, or the risk level is in the reduction list of the main decision structure, that is, the risk has moderate benefits but should be reduced below $U$.

Wilson’s upper bound $U = 10^{-3}$ means that the traffic accident risk level $R \leq U$ should be subject to intensive RCB study for justification; if the risk is justified, then it is reluctantly accepted; if the risk is not justified, then it must be reduced until another justification or until it is below the lower bound $L$. 

Wilson showed that the lower bound $L = 10^{-6}/(\text{year, individual})$ is equivalent to the risk level of any one of the following activities: smoking three U.S. cigarettes (cancer, heart disease), drinking 0.5 liters of wine (cirrhosis of the liver), visiting New York or Boston for two days (air pollution), and spending six minutes in a canoe (accident). The lower bound $L = 10^{-5}$ by Comar can be interpreted in a similar way: for instance, it is comparable to drinking five liters of wine per year.

Spangler claims that the Wilson's annual lower bound $L = 10^{-6}$ is more acceptable than Comar's bound $L = 10^{-5}$ for the following situations [5]:

1. Whenever the risk is involuntary.
2. Whenever there is a substantial band of uncertainty in estimating risk at such low levels.
3. Whenever the risk has a high degree of expert and public controversy.
4. Whenever there is a reasonable prognosis that new safety information is more likely to yield higher-than-current best estimates of the risk level rather than lower estimates.

Accumulation problems for lower bound risks. The lower bound $L = 10^{-6}/(\text{year, individual})$ would not be suitable if the risk level were measured not per year but per operation. For instance, the same operation may be performed repetitively by a dangerous forging press. The operator of this machine may think that the risk per operation is negligible because there is only one chance in one million of an accident, so he removes safety interlocks to speed up the operation. However, more than ten thousand operations may be performed during a year, yielding a large annual risk level, say $10^{-2}$, of injury. Another similar accumulation may be caused by multiple risk sources or by risk exposures to a large population; if enough negligible doses are added together, the result may eventually be significant [11]; if negligible individual risks of fatality are integrated over a large population, a sizable number of fatalities may occur.

**ALARA—As low as reasonably achievable.** A decision structure similar to the ones described above is recommended by ICRP (International Commission on Radiological Protection) Report No. 26 for individual-related radiological protection [10]. Note that population-related protection is not considered.

1. Justification of practice: No practice shall be adopted unless its introduction produces a positive net benefit.
2. Optimization of protection: All exposures shall be kept as low as reasonably achievable (i.e., ALARA), economic and social factors being taken into account.
3. The radiation doses to individuals shall not exceed the dose equivalent limits recommended for the appropriate circumstances by ICRP.

The third statement corresponds to upper bound $U$ in the three-layer decision structure. The ICRP report lacks lower bound $L$, however, and there is a theoretical chance that the risk would be overreduced to any small number, as long as it is feasible to do so by ALARA.

The NRC adoption of ALARA radiation protection standards for the design and operation of light water reactors in May 1975 interpreted the term as low as reasonably achievable to mean as low as is reasonably achievable taking into account the state of technology and the economics of improvements, in relation to benefits, to public health and safety and other societal and socioeconomic considerations, and in relation to the utilization of atomic energy in the public interest [10]. Note here that the term benefits does not denote
the benefits of atomic energy but reduction of risk levels; *utilization of atomic energy in the public interest* denotes the benefits in the usual sense for RCB analyses.

For population-related protection, the NRC proposed a conservative value of $1000 per total body person-rem (collective dose for population risk) averted for the risk/cost evaluations for ALARA [10]. The value of $1000 is roughly equal to $7.4 million per fatality averted if one uses the ratio of 135 lifetime fatalities per million person-rem's. This ALARA value established temporarily by the commission is substantially higher than the equity value of $250,000 to $500,000 per fatality averted referenced by other agencies in risk-reduction decisions. (The lower equity values apply, of course, to situations where there is no litigation, i.e., to countries other than the United States.)

**De minimis risk.** The concept of de minimis risk is discussed in the book edited by Whipple [21]. A purpose of de minimis risk investigation is a justification of a lower bound \( L \) below which no active study of the risk, including ALARA or RCB analyses, is required. Davis, for instance, describes in Chapter 13 of the book how the law has long recognized that there are trivial matters that need not concern it; the maxim *de minimis non curat lex*, "the law does not concern itself with trifles," expresses that principle [11]. (In practice, of course, the instance of a judge actually dismissing a lawsuit on the basis of triviality is a very rare event.) She suggests the following applications of de minimis risk concepts [10].

1. For setting regulatory priorities
2. As a "floor" for ALARA considerations
3. As a cut-off level for collective dose assessments
4. For setting outer boundaries of geographical zones
5. As a floor for definition of low-level wastes
6. As a presumption of triviality in legal proceedings
7. To foster administrative and regulatory efficiency
8. To provide perspective for public understanding, including policy judgments

Some researchers of the de minimis say that \( 10^{-6} \) (year, individual) risk is trivial, acceptable, or negligible and that no more safety investment or regulation is required at all for systems with the de minimis risk level. Two typical approaches for determining the de minimis radiation level are comparison with background radiation levels and detectability of radiation [11]. Radiation is presumed to cause cancers, and the radiation level can be converted to a fatal cancer level.

**ALARA versus de minimis.** Cunningham [10] noted:

We have a regulatory scheme with upper limits above which the calculated health risk is generally unacceptable. Below these upper limits are various specific provisions and exemptions involving calculated risks that are considered acceptable based on a balancing of benefits and costs, and these need not be considered further. Regulatory requirements below the upper limits are based on the ALARA principle, and any risk involved is judged acceptable given not only the magnitude of the health risk presented but also various social and economic considerations. A de minimis level, if adopted, would provide a regulatory cutoff below which any health risk, if present, could be considered negligible. Thus, the de minimis level would establish a lower limit for the ALARA range of doses.

The use of ALARA-type procedures can provide a basis for establishing an explicit standard of de minimis risk beyond which no further analysis of costs and benefits need be employed to determine the acceptability of risk [10]; in this context, the de minimis
risk is a dependent variable in the ALARA procedure. An example of such a procedure is the cost-benefit guideline of $1000 per total person-rem averted (see Figure 1.25). Such a determination of the de minimis risk level by ALARA, however, would yield different lower bounds for different risk sources; this blurs the three-layer decision structure with a universal lower bound that says that no more ALARA is required below the constant bound even if a more cost-effective alternative than the $1000 guideline is available.

![Figure 1.25. De minimis risk level determined by ALARA.](image)

### 1.5.4 Goals for Normal Activities

**Lower bound goals.** Examples of quantitative design goals for lower bound $L$ for a light-water-cooled power reactor are found in Title 10 of CFR Part 50, Appendix I [10]. They are expressed in terms of maximum permissible annual individual doses:

1. Liquid effluent radioactivity: 3 millirems for the whole body and 10 millirems to any organ.
2. Gaseous effluent radioactivity: 5 millirems to the whole body and 15 millirems to the skin.
3. Radioactive iodine and other radioactivity: 15 millirems to the thyroid.

If one uses the ratio of 135 lifetime fatalities per million person-rem, then the 3 mrem whole-body dose for liquid effluent radioactivity computes to a probability of four premature fatalities in 10 million. Similarly, 5 mrem of whole-body dose for gaseous effluent radioactivity yields a probability of $6.7 \times 10^{-7}$/lifetime, individual) fatality per
year of exposure. These values comply with the individual risk lower bound $L = 10^{-6}/\text{year, individual}$ proposed by Wilson or by the de minimis risk.

**Upper bound goals.** According to the current radiation dose rate standard, a maximum allowable annual exposure to individuals in the general population is 500 mrems/year, excluding natural background and medical sources [11]. As a matter of fact, the average natural background in the United States is 100 mrem per year, and the highest is 310 mrem per year. The 500 mrems/year standard yields a probability for a premature fatality of $6.7 \times 10^{-5}$. This can be regarded as an upper bound $U$ for an individual.

If the Wilson's bounds are used, the premature fatality likelihood lies in the middle layer, $L = 10^{-6} < 6.7 \times 10^{-5} < U = 10^{-3}$. Thus the risk must be justified; otherwise, the risk should be reduced below the lower bound. A possibility is to reduce the risk below the maximum allowable exposure by using a safety-cost trade-off value such as the $1000 \text{ person-rem}$ in the NRC's ALARA concept [10].

A maximum allowable annual exposure to radiological industrial workers is 5 rems per year [11], which is much less stringent than for individuals in the general population. Thus we do have different upper bounds $U$'s for different situations.

Having an upper bound goal as a necessary condition is better than nothing. Some unsafe alternatives are rejected as unacceptable; the chance of such a rejection is increased by gradually decreasing the upper bound level. A similar goal for the upper bound has been specified for NO$_2$ concentrations caused by automobiles and factories. Various upper bound goals have been proposed for risks posed by airplanes, ships, automobiles, buildings, medicines, food, and so forth.

### 1.5.5 Goals for Catastrophic Accidents

**Lower bound goals.** Some lower bound goals for catastrophic accidents are stated qualitatively. A typical example is the qualitative safety goals proposed by the NRC in 1983 [22,10]. The first is related to individual risk, while the second is for population risk.

1. **Individual risk:** Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.

2. **Population risk:** Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

The NRC proposal also includes quantitative design objectives (QDOs).

1. **Prompt fatality QDO:** The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

2. **Cancer fatality QDO:** The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.
3. **Plant performance objective:** The likelihood of a nuclear reactor accident that results in a large-scale core melt should normally be less than 1 in 10,000 per year of reactor operation.

4. **Cost-benefit guideline:** The benefit of an incremental reduction of societal mortality risks should be compared with the associated costs on the basis of $1000 per person-rem averted.

   The prompt (or accident) fatality rate from all causes in the United States in 1982 was $4 \times 10^{-4}$ per year; 93,000 deaths in a population of 231 million. At 0.1\% of this level, the prompt fatality QDO becomes $4 \times 10^{-7}$ per year, which is substantially below the lower bound $L = 10^{-6}$ for an individual [10]. In 1983, the rate of cancer fatalities was $1.9 \times 10^{-3}$. At 0.1\% of this background rate, the second QDO is $1.9 \times 10^{-6}$, which is less limiting than the lower bound.

   On August 4, 1986, the NRC left unchanged the two proposed qualitative safety goals (individual and population) and the two QDOs (prompt and cancer). It deleted the plant performance objective for the large-scale core melt. It also deleted the cost-benefit guideline. The following guideline was proposed for further examination:

5. **General performance guideline:** Consistent with the traditional defense-in-depth approach and the accident mitigation philosophy requiring reliable performance of containment systems, the overall mean frequency of a large release of radioactive materials to the environment from a reactor accident should be less than $10^{-6}$ per year of reactor operation.

   The general performance guideline is also called an FP (fission products) large release criteria. Offsite property damage and erosion of public confidence by accidents are considered in this criteria in addition to the prompt and cancer fatalities.

   The International Atomic Energy Agency (IAEA) recommended other quantitative safety targets in 1988 [23,24]:

   1. For existing nuclear power plants, the probability of severe core damage should be below $10^{-4}$ per plant operating year. The probability of large offsite releases requiring short-term responses should be below $10^{-5}$ per plant operating year.

   2. For future plants, probabilities lower by a factor of ten should be achieved.

   The future IAEA safety targets are comparable with the plant performance objective and the NRC general performance guideline.

**Risk-aversion goals.** Neither the NRC QDOs nor the IAEA safety targets consider risk aversion explicitly in severe accidents; two accidents are treated equivalently if they yield the same expected numbers of fatalities, even though one accident causes more fatalities with a smaller likelihood. A Farmer curve version can be used to reflect the risk aversion. Figure 1.26 shows an example. It can be shown that a constant curve of expected number of fatalities is depicted by a straight line on a log $f$ versus log $x$ graph, where $x$ is the number of fatalities and $f$ is the frequency density around $x$.

Fatality excess curves have been proposed in the United States; more indirect curves such as dose excess have been proposed in other countries, although the latter can, in theory, be transformed into the former. The use of dose excess rather than fatality excess seems
Sec. 1.5  Safety Goals

Figure 1.26. Constant fatality versus risk-aversion goal in terms of Farmer curves.

preferable in that it avoids the need to adopt a specific dose-risk correlation, to make extrapolations into areas of uncertainty, and to use upper limits rather than best estimates [11].

Risk profile obtained by cause-consequence diagram. Cause-consequence diagrams were invented at the Risø Laboratories in Denmark. This technology is a marriage of event trees (to show consequences) and fault trees (to show causes), all taken in their natural sequence of occurrence. Figure 1.27 shows an example. Here, construction starts with the choice of a critical initiating event, motor overheating.

The block labeled A in the lower left of Figure 1.27 is a compact way of showing fault trees that consist of component failure events (motor failure, fuse failure, wiring failure, power failure), logic gates (OR, AND), and state-of-system events (motor overheats, excessive current to motor, excessive current in circuit). An alternative representation (see Chapter 4) of block A is given in Figure 1.28.

The consequence tracing part of the cause-consequence analysis involves taking the initiating event and following the resulting chain of events through the plant. At various steps, the chains may branch into multiple paths. For example, the motor overheating event may or may not lead to a motor cabinet local fire. The chains of events may take alternative forms, depending on conditions. For example, the progress of a fire may depend on whether a traffic jam prevents the fire department from reaching the fire on time.

The procedure for constructing the consequence scenario is first to take the initiating event and each later event by asking:

1. Under what conditions does this event lead to further events?
2. What alternative plant conditions lead to different events?
3. What other components does the event affect? Does it affect more than one component?
4. What further event does this event cause?

The cause tracing part is represented by the fault tree. For instance, the event “motor overheating” is traced back to two pairs of concatenated causes: (fuse failure, wiring failure) and (fuse failure, power failure).
Figure 1.27. Example of cause-consequence diagram.
We now show how the cause-consequence diagram can be used to construct a Farmer curve of the probability of an event versus its consequence. The fault tree corresponding to the top event, "motor overheats," has an expected number of failures of $P_0 = 0.088$ per 6 months, the time between motor overhauls. There is a probability of $P_1 = 0.02$ that the overheating results in a local fire in the motor cabinet. The consequences of a fire are $C_0$ to $C_4$, ranging from a loss of $1000$ if there is equipment damage with probability $P_0(1 - P_1)$ to $5 \times 10^7$ if the plant burns down with probability $P_1 P_2 P_3 P_4$. The downtime loss is estimated at $1000$ per hour; thus the consequences in terms of total loss are

$$C_0 = 1000 + (2)(1000) = 3000$$

$$C_1 = 15,000 + (24)(1000) = 39,000$$, and so forth

Assume the probabilities $P_0 = 0.088$, $P_1 = 0.02$, $P_2 = 0.133$, $P_3 = 0.043$, and $P_4 = 0.065$. Then a risk calculation is summarized as follows.

<table>
<thead>
<tr>
<th>Event</th>
<th>Total Loss</th>
<th>Event Probability</th>
<th>Expected Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_0$</td>
<td>$3000$</td>
<td>$P_0(1 - P_1) = 0.086$</td>
<td>$258$</td>
</tr>
<tr>
<td>$C_1$</td>
<td>$39,000$</td>
<td>$P_0 P_1(1 - P_2) = 1.53 \times 10^{-3}$</td>
<td>$60$</td>
</tr>
<tr>
<td>$C_2$</td>
<td>$1.744 \times 10^4$</td>
<td>$P_0 P_1 P_2(1 - P_3) = 2.24 \times 10^{-4}$</td>
<td>$391$</td>
</tr>
<tr>
<td>$C_3$</td>
<td>$2 \times 10^7$</td>
<td>$P_0 P_1 P_2 P_3(1 - P_4) = 9.41 \times 10^{-6}$</td>
<td>$188$</td>
</tr>
<tr>
<td>$C_3 + C_4$</td>
<td>$5 \times 10^7$</td>
<td>$P_0 P_1 P_2 P_3 P_4 = 6.54 \times 10^{-7}$</td>
<td>$33$</td>
</tr>
</tbody>
</table>

The total expected loss is thus

$$258 + 60 + 391 + 188 + 33 = 930/6 \text{ months} = 1860/\text{year}$$

Figure 1.28. Alternative representation of "Motor Overheats" event.
Figure 1.29 shows the Farmer risk curve, including the $300 expected risk-neutral loss line per event. This type of plot is useful for establishing design criteria for failure events such as "motor overheats," given their consequence and an acceptable level of risk.

1.5.6 Idealistic Versus Pragmatic Goals

The Wilson's lower bound goal $L = 10^{-6}$/year, individual) is reasonable either from idealistic or pragmatic viewpoints when a relatively small population is affected by the risk. A typical example of such a population would be a crew of the U.S. space shuttle. When a large number of people are exposed to the risk, however, the lower bound is not a suitable measure for the unconditional acceptance of the risk, that is, the Wilson's lower bound is not necessarily a suitable measure for the population risk (see Figure 1.11).

A randomized, perfect crime. Suppose that a decorative food additive* causes a $10^{-6}$ fatal cancer risk annually for each individual in the U.S. population, and that the number $x$ of cancer fatalities over the population by the additive is distributed according to a binomial distribution.

$$
\Pr\{x\} = \binom{n}{x} p^x (1 - p)^{n-x}, \quad p = 10^{-6}, \quad n = 235 \times 10^6 \quad (1.30)
$$

The expected number $E[x]$ of cancer fatalities per year is

$$
E[x] = np = 235 \quad (1.31)
$$

while the variance $V[x]$ of $x$ is given by

$$
V[x] = np(1 - p) \simeq np = E[x] = 235 \quad (1.32)
$$

By taking a 1.95 sigma interval, we see that it is 95% certain that the food additive causes from 205 to 265 fatalities. In other words, it is 97.5% certain that the annual cancer fatalities would exceed 205. The lower bound $L = 10^{-6}$ or the de minimis risk, when applied to the population risk, claims that this number is so small compared with two million annual deaths in the United States that it is negligible; $235/2,000,000 \simeq 0.0001$: among 10,000 fatalities, only one is caused by the additive.

---

*If the food additive saved human lives, we would have a different problem of risk-benefit trade-off.
In the de minimis theory, the size of the population at risk does not explicitly influence the selection of the level of the lower bound risk. Indeed, the argument has been made that it should not be a factor. The rationale for ignoring the size (or density) of the population at risk when setting standards should be examined in light of the rhetorical question posed by Milvy [3]:

Why should the degree of protection that a person is entitled to differ according to how many neighbors he or she has? Why is it all right to expose people in lightly populated areas to higher risks than people in densely populated ones?

As a matter of fact, individual risk is viewed from the vantage point of a particular individual exposed; if the ratio of potential fatalities to the size of the population remains a constant, then the individual risk remains at the same level even if the population becomes larger and the potential fatalities increase. On the other hand, population risk is a view from a risk source or a society that is sensitive to the increase of fatalities.

Criminal murders, in any country, are crimes. The difference between the 205 food additive murders and criminal murders is that the former are performed statistically. A criminal murder requires that two conditions hold: intentional action to murder and evidence of causal relations between the action and the death. For the food additive case, the first condition holds with a statistical confidence level of 97.5%. However, the second condition does not hold because the causal relation is probabilistic—1 in 10,000 deaths in the United States. The 205 probabilistic deaths are the result of a perfect crime.

Let us now consider the hypothetical progress of a criminal investigation. Assume that the fatal effects of the food additive can be individually traced by autopsy. Then the food company using the additive would have to assume responsibility for the 205 cancer fatalities per year: there could even be a criminal prosecution. We see that for the food additive case there is no such concept as de minimis risk, acceptable risk level, or negligible level of risk unless the total number of fatalities caused by the food additive is made much smaller than 205.

**Necessity versus sufficiency problem.** A risk from an alternative is rejected when it exceeds the upper bound level $U$, which is all right because the upper bound goal is only a necessary condition for safety. Alternatives satisfying this upper bound goal would not be accepted if they neither satisfied the lower bound goal nor were justified by RCB analyses or ALARA. A risk level is subject to justification processes when it exceeds the lower bound level $L$, which is also all right because the lower bound goal is also regarded as a necessary condition for exemption from justification.

Many people in the PRA field, however, incorrectly think that considerably higher lower bound goals and even upper bound goals constitute sufficient conditions. They assume that safety goals are solutions for problems of how safe is safe enough, acceptable level of risks, and so forth. This failure to recognize the necessity feature of the lower and upper bound goals has caused confusion in PRA interpretations, especially for population risks.

**Regulatory cutoff level.** An individual risk of $10^{-6}/\text{year, individual}$ is sufficiently close to the idealistic, Platonic, lower bound sufficiency condition, that is, the de minimis risk. Such a risk level, however, is far from idealistic for risks to large populations. The lower bound $L$ as a de minimis level for population risks must be a sufficiently small fractional number; less than one death in the entire population per year. If some risk level greater than this de minimis level is adopted as a lower bound, the reason must come from factors outside the risk itself. A pragmatic lower bound is called a regulatory cutoff level.
A pragmatic cutoff level is, in concept, different from the de minimis level: 1) the regulatory cutoff level is a level at or below which there are no regulatory concerns, and 2) a de minimis level is the lower bound level $L$ at or below which the risks are accepted unconditionally. Some risks below the regulatory cutoff level may not be acceptable, although the risks are not regulated—the risks are only reluctantly accepted as a necessary evil. Consequently, the de minimis level for the population risk is smaller than the regulatory cutoff level currently enforced.

Containment structures with 100-foot-thick walls, population exclusion zones of hundreds of square miles, dozens of standby diesel generators for auxiliary feedwater systems, and so on are avoided by regulatory cutoff levels implicitly involving cost considerations [15].

Milvy [3] claims that a $10^{-6}$ lifetime risk to the U.S. population is a realistic and prudent regulatory cutoff level for the population risk. This implies 236 additional deaths over a 70-year interval (lifetime), and 3.4 deaths per year in the population of 236 million. This section briefly overviews a risk-population model as the regulatory cutoff level for chemical carcinogens.

**Constant likelihood model.** When the regulatory cutoff level is applied to an individual, or a discrete factory, or a small community population that is uniquely at risk, its consequences become extreme. A myriad of society’s essential activities would have to cease. Certainly the X-ray technician and the short-order cook exposed to benzopyrene in the smoke from charcoal-broiled hamburgers are each at an individual cancer risk considerably higher than the lifetime risk of $10^{-6}$. Indeed, even the farmer in an agricultural society is at a $10^{-3}$ to $10^{-4}$ lifetime risk of malignant melanoma from pursuing his trade in the sunlight. The $10^{-6}$ lifetime criterion may be appropriate when the whole U.S. population is at risk, but to enforce such a regulatory cutoff level when the exposed population is small is not a realistic option. Thus the following equation for regulatory cutoff level $L_1$ is too strict for a small population

$$L_1 = 10^{-6}/\text{lifetime} \quad (1.33)$$

**Constant fatality model.** On the other hand, if a limit of 236 deaths is selected as the criterion, the equation for cutoff level $L_2$ for a lifetime is

$$L_2 = (236/x)/\text{lifetime}, \quad x: \text{population size} \quad (1.34)$$

This cutoff level is too risky for a small population size of several hundred.

**Geometric mean model.** We have seen that, for small populations, $L_1$ from the constant likelihood model is too strict and that $L_2$ from the constant fatality model is too risky. On the other hand, the two models give the same result for the whole U.S. population. Multiplying the two cutoff levels and taking the square root yields the following equation, which is based on a geometric mean of $L_1$ and $L_2$.

$$L = 0.015/\sqrt{x} \quad (1.35)$$

Using the equation with $x = 100$, the lifetime risk for the individual is $1.5 \times 10^{-3}$ and the annual risk is $2.14 \times 10^{-5}$. This value is nearly equal to the lowest annual fatal occupational rate from accidents that occur in the finance, insurance, and real estate occupational category. The geometric mean risk-population model plotted in Figure 1.30 is deemed appropriate only for populations of 100 or more because empirical data suggest that smaller populations are not really relevant in the real world, in which environmental
Sec. 1.5  ■  Safety Goals

and occupational carcinogens almost invariably expose groups of more than 100 people. Figure 1.31 views the geometric mean model from expected number of lifetime fatalities rather than lifetime fatality likelihood.

Figure 1.30. Regulatory cutoff level from geometric mean risk-population model.

Figure 1.31. Geometric mean model viewed from lifetime fatalities.

Past regulatory decisions. Figure 1.32 compares the proposed cutoff level $L$ with the historical data of regulatory decisions by the Environmental Protection Agency. Solid squares represent chemicals actively under study for regulation. Open circles represent the decision not to regulate the chemicals. The solid triangles provide fatal accident rates
for: 1) private sector in 1982; 2) mining; 3) finance, insurance, and real estate; and 4) all. The solid line, \( L = 0.28 x^{-0.47} \), represents the best possible straight line that can be drawn through the solid squares. Its slope is very nearly the same as the slope of the geometric mean population-risk equation, \( L = 0.015 x^{-1/2} \), also shown in the figure.

Figure 1.32. Regulatory cutoff level and historical decisions.

Although the lines are nearly parallel, the line generated from the data is displaced almost one and a half orders of magnitude above the risk-population model. This implies that these chemicals lie above the regulatory cutoff level and should be regulated. Also consistent with the analysis is the fact that ten of the 16 chemicals or data points that fall below the geometric mean line are not being considered for regulation. The six data points that lie above the geometric mean line, although not now being considered for regulation, in fact do present a sufficiently high risk to a sufficiently large population to warrant regulation.

The fact that the slopes are so nearly the same also seems to suggest that it is recognized—although perhaps only implicitly—by the EPA’s risk managers that the size of the population at risk is a valid factor that has to be considered in the regulation of chemical carcinogens.

1.5.7 Summary

Risk goals can be specified on various levels of system hierarchy in terms of a variety of measures. The safety goal on the top level is a starting point for specifying the goals on the lower levels. PRAM procedures become more useful when a hierarchical goal system is established. A typical decision procedure with safety goals forms a three-layer structure. The ALARA principle or RCB analysis operates in the second layer. The de minimis risk gives the lower bound goal. The upper bound goal rejects risks without overriding benefits. Current upper and lower bound goals are given for normal activities and catastrophic accidents. When a risk to a large population is involved, the current lower bound goals should be considered as pragmatic goals or regulatory cutoff levels. The geometric mean model explains the behavior of the regulatory cutoff level as a function of population size.
REFERENCES


Basic Risk Concepts

1.1. Give a definition of risk. Give three concepts equivalent to risk.

1.2. Enumerate activities for risk assessment and risk management, respectively.

1.3. Explain major sources of debate in risk assessment and risk management, respectively.

1.4. Consider a trade-off problem when fatality is measured by monetary loss. Draw a schematic diagram where outcome probability and cost are represented by horizontal and vertical axes, respectively.

1.5. Pictorialize relations among risk, benefits, and acceptability.

1.6. Consider a travel situation where $1000 is stolen with probability 0.5. For a traveler, a $750 insurance premium is equivalent to the theft risk. Obtain a quadratic loss function $s(x)$ with normalizing conditions $s(0) = 0$ and $s(1000) = 1$. Calculate an insurance premium when the theft probability decreases to 0.1.

1.7. A Bayesian explanation of outcome severity overestimation is given by (1.19). Assume $\Pr\{10|\text{Defect}\} > \Pr\{10|\text{No defect}\}$. Prove:
   (a) The a posteriori probability of a defect conditioned by the occurrence of a ten-fatality accident is larger than the a priori defect probability
   
   $$\Pr\{\text{Defect}|10\} > \Pr\{\text{Defect}\}$$

   (b) The overestimation is more dominant when the a priori probability is smaller, that is, the following ratio increases as the a priori defect probability decreases.
   
   $$\Pr\{\text{Defect}|10\}/\Pr\{\text{Defect}\}$$

1.8. Explain the following concepts: 1) hierarchy of safety goals, 2) three-layer decision structure for risk acceptance, 3) ALARA, 4) de minimis risk, 5) geometric mean model for a large population risk exposure.

1.9. Give an example of qualitative and quantitative safety goals for catastrophic accidents.