Risk Assessment & Management

Themes
1. Concept/Types of Risk
2. Probabilistic Risk Assessment
3. Social Risk Management Considerations

Concept/Types of Risk

The notion of risk is basically a combination of two concepts: probability and severity. That is, we decide how risky something is by asking two questions:

- How likely is this to happen? (probability)
- How bad would it be if this did happen? (severity)

Before going further, let us clarify a few terms. A hazard is anything potentially costly, harmful, or undesirable. Hazards lead to risks. The connection between hazard and risk is an event – a situation in which someone/thing is exposed to the hazard. It is important not to confuse these terms. A pot of boiling water is a hazard, since it could cause harm. How risky is it? We cannot say, without information about who/what is exposed to it. If we specify an event, such as a person bumping the pot (and getting burned), then we can assess the probability and severity, and from these the risk (note that both are required; either alone is insufficient, i.e., uncertainty does not necessarily mean risk).

Risk can be assessed either quantitatively or qualitatively. If both the probability and severity can be quantified, the risk is simply the product: risk = probability * severity. For example, if the probability of a computer server “crashing” in a 24-hour period is $10^{-6}$, and if the cost of a crash is estimated to be $2,000,000 (for lost revenue while the system is down, plus repairs), then the risk of relying upon such a server is about $2 per day. This could be compared with the cost risk of an alternative.

Assessing risks is not always straightforward, however. The probability or severity of an event may not be known (e.g., the probability that your car will break down tomorrow), or not agreed-upon (e.g., the severity of global warming). Many risks may be associated with a given hazard. Risks associated with a complex system, such as a nuclear power plant, may involve long chains of events. For all these reasons, deciding exactly what to include, and how to treat it, can be difficult.
Finally, there are many different types of risk – as many as there are values that can be threatened. Among the most prominent types are safety, cost, schedule, technical, and political risk, and most decisions involve more than one of these. An important part of risk management is deciding which types of risk to assess, and how they should be compared to make decisions.

In the following sections we will introduce probabilistic risk assessment (PRA), a formal method for technical risk analysis, and we will discuss social considerations, such as risk perception and acceptability.

**Probabilistic Risk Assessment**

Probabilistic risk assessment (PRA) is a quantitative procedure used to evaluate technical risks. The basic process involves five steps:

1. Identify hazards and initiating events
2. Identify mitigating safety measures
3. Trace possible chains of events
4. Quantify all individual probabilities and severities
5. Aggregate probabilities and severities, and calculate risks

A principal component of PRA is reliability analysis. *Reliability* is simply a different form (the reciprocal) of probability of failure. Thus it is related to risk. (Note: it is a common misconception that reliability is simply risk in a different form. This is not the case, because reliability does not contain severity information.) For nested systems, the reliability of each subsystem must be assessed independently, and then all of these values aggregated to determine overall system reliability.* As systems grow in complexity, accounting for the effects of various combinations of subsystem failures quickly becomes very complicated. Consequently, methods such as fault and event trees have been developed to facilitate such analysis. These are introduced below.

The rest of this section presents a formal procedure for conducting PRA.† Specified in ten steps, it addresses more details than the basic description above, but it is fundamentally equivalent. We will discuss each step in turn.

---

* This aggregation is governed by the mathematics of logical combination (e.g., Boolean Algebra for binary combinations), which uses operators such as “AND” and “OR” for elements in series or in parallel.
1. **Methodology Definition**

The first step in preparing a PRA is to review the analytical options: using computer programs, consulting experts, etc. The requirements for the PRA and the advantages and disadvantages of each analytical option should then be considered, and the most cost-effective option selected.

2. **Familiarization and Information Assembly**

Next, it is important to become familiar with the system or process under consideration. The physical layout, standard procedures, safety measures, etc. should all be investigated. It is essential to understand how things are supposed to work, what could go wrong, and what might happen if it did. It is also valuable to review the details of any failures that have occurred in the past. All of this information should be organized and documented to facilitate future review and provide a solid foundation for the PRA.

3. **Identification of Initiating Events**

Once the system is understood, it is time to build a list of internal initiating events – abnormal events within the system, that could result in hazard exposure if not properly remedied. There are a number of ways to approach this, from “what-if” brainstorming to Failure Mode and Effects Analysis (FMEA). The important thing is to identify as many plausible internal hazards and associated events as possible. For engineering systems, a common approach is to identify hazards with barriers, and the threats they pose to those barriers, but this is not always necessary.

If the list of initiating events becomes extensive, it would probably be wise to group similar events together. For example, categories can be defined for all events that break the same barrier, contribute to the same risk, or require the same corrective actions. This will simplify the rest of the analysis, focusing concentration on significant categories instead of redundant events.

4. **Sequence or Scenario Development**

The next step is to investigate the consequences of internal the initiating events. This is usually achieved through event tree analysis. An event tree is a diagram depicting all the possible consequences of an initiating event. Such a tree is created by starting with the initiating event and identifying all of its relevant consequences, then systematically treating each consequence as a new event and identifying its consequences, and so on. This structure of possible consequence events branching out to more possible events at
each level forms a “tree.” Although they can quickly grow large, trees are valuable because they enable us to trace causal paths of events.

A simple example event tree is presented in Figure 3.2.1. The initiating event is a fire, for which we identify two possible consequences: activate the sprinkler system and call the fire department. We begin with the sprinklers as the next event level. Here we identify two more possible consequences: the sprinklers either succeed or fail. For either result we then go to the next branch, the fire fighters, for which we also identify succeed or fail consequences. (This branch is attached to both branches from the sprinkler event, because whether the sprinklers succeed or not, the fire company is called.) At this point the tree stops, because there are no more consequences to include.

To complete the tree, we now label all of the final outcomes. If the sprinklers succeed, then if the fire fighters succeed the system will be OK, or if the fire fighters fail there will be only partial damage. However if the sprinklers fail to begin with, then if the fire fighters succeed there still will be partial damage, or if the fire fighters also fail the system will be destroyed. Thus we can see that an initiating event of a fire could lead to any of three ultimate consequences – the system could be OK, partially damaged, or destroyed – and we can see the paths, or event sequences, that lead to each.†

This is only part of the functionality of event trees. In later steps of the PRA, we will return to each event tree and define the branch probabilities (in this example, these would be the sprinklers’ and fire fighters’ probabilities of success), and then aggregate them to calculate the likelihood of each outcome. Finally, we will quantify the severity of each

---

* Example event tree courtesy of Relex Software [http://www.event-tree.com/].
† Note: the two kinds of partial damage could just as easily have been distinguished, leading to four ultimate outcomes. Determining the appropriate level of resolution is part of the “art” of risk analysis.
outcome, and determine the overall risks. But at this point, the goal is just to trace the paths of possible consequences from initiating events. To complete Step 4, such an event tree must be created for each initiating event identified in Step 3.

5. System Analysis

In many cases, event trees contain important branch points, such as where a critical safeguard may or may not function, for which we do not have much information. In the example above, we might be concerned with exactly how likely the sprinkler system is to succeed. To gain such information, we must conduct internal system analysis. A useful approach in many situations is fault tree analysis. A fault tree is similar to an event tree in that it starts with an event, but instead following the consequences, it traces the causes.

Figure 3.2.1 presents an example fault tree for the sprinkler system. It begins with the problem we wish to analyze, known as the “top” fault or event, which in this case is the sprinklers failing to extinguish the fire. What could cause this? The sprinklers never get activated, or they are activated but fail to operate. These “triggering” events are linked to the top fault with an “OR-gate” because it only takes one or the other to cause the fault. Now we add a branch tracing their causes. The sprinklers never get activated if the automatic sensors fail and no manual activation occurs. These are linked through an “AND-gate” because it takes both of them to cause the fault. Finally, the sprinklers fail to operate, even if activated, if water does not reach them OR if their valves fail to open.

![Figure 3.2.2: Fault Tree](image-url)
Obviously we could continue the tree further, listing causes for each of these third-level triggering events, but at some point we have to stop. (This point is a judgment call; it depends on what is of interest and what information is available.) We call the triggering events at the bottom (or at the ends of the branches, since the tree could be oriented in any direction) “basic events” or “root causes.” We assign probabilities to each root cause, and then combine these probabilities, to get probability of the event one level up. We proceed in this way, level by level, until we finally have the probability of the top fault. Now we can update our event trees with this improved information.

6. Internal Events External to the Facility

This step simply takes into consideration any events that originate within the system but then spread beyond the facility boundaries. Some examples might be internal fires, floods, or energy discharges. In most cases, there will be few events of this type, but any that are included should be analyzed just like the internal events in Steps 3-5.

7. External Events

Here, we simply consider the last category of events, those originating outside the system, such as storms, seismic events, transportation events, etc. As before, any new events that are included should be analyzed just like the internal events in Steps 3-5.

8. Dependent Failure Considerations

A common risk management practice is the installation of redundant systems. This increases reliability by creating multiple success paths – but only as long as the systems are truly independent. If there is any dependency, a failure in one unit could compromise another. There is sometimes a risk of such failure coupling even in systems thought to be independent, if they share the same operating environment or have functional or spatial links. Accordingly, it is important to carefully look for elements that could be prone to common-cause failures, and to make sure that they (and their potential dependencies) are explicitly incorporated in fault and event trees wherever applicable.

9. Failure Data Analysis

The next step is to obtain failure data for all of the events listed in all fault and event trees. There are a variety of sources of failure data. Past experiences are usually best (if any failures in this, or other similar systems, have occurred), but some values must be estimated from generic failure data, or based on expert opinion. Data should also be obtained and included for outages due to test, repair, and maintenance.
10. Quantification

To complete the PRA, the information from Step 9 is applied to fully quantify all fault and event tree sequences. These are then reduced and combined to obtain probability and severity information for the desired system elements, operations, and events.

For example, let us return to the event tree developed in Step 4. Suppose that the data obtained in Step 9 included the following probability and severity information, to be added to the event tree (Figure 3.2.3):

- P(sprinkler system success): 0.8
- P(fire dept. success | sprinkler success): 0.95
- P(fire dept. success | sprinkler failure): 0.5
- Cost(fire handled OK): –$1,000
- Cost(partial damage): –$500,000
- Cost(system destroyed): –$3,500,000

![Figure 3.2.3: Event Tree With Quantification](image)

Now it is simply a matter of calculation: the overall probability of an OK outcome (only $1000 damage) is (0.9)(0.95) = 85.5%; the overall probability of a Partial Damage outcome ($500k damage) is (0.9)(0.05) + (0.1)(0.7) = 11.5%; and the overall probability of system destruction ($3.5M damage) is (0.1)(0.3) = 3%. Then, combining the probability and severity information, we can calculate that the overall average risk of fire damage: (.855)(−$1,000) + (.115)(−$500,000) + (.03)(−$3,500,000) = −$163,355.

Finally, if any risk levels are not acceptable, the fault and event trees can be used to identify problem areas and/or common sequences leading to undesirable outcomes. These
can then be targeted for risk management efforts. For example, if the risk calculated above was deemed too high, the sprinkler system could be targeted for improvement (to increase its probability of success). Note that additional system analysis (Step 5) may be required to determine exactly how to achieve the desired improvements.

**Social Risk Management Considerations**

By this point, you should be familiar with risk and related concepts, and you should understand how to conduct a probabilistic risk assessment (PRA) to gain information about event sequences’ probabilities, severities, and overall risk levels. This is an excellent start. In the real world, however, managing risks frequently requires more than a series of calculations indicating something is sufficiently “safe.” It is not uncommon for people to demand additional safety precautions, or to decide a project is simply too risky, despite the results of quantitative analysis. This section addresses these issues.

PRA or similar analysis, if properly conducted on a suitable subject, does provide a valid, consistent measure of risk, but risk perception and risk acceptability are also important. Risk perception is the human internalization of risk information. Our perceptions shape all of our decisions about risky activities, from crossing a street to making a financial investment. Unfortunately for technical analysts, however, both our perceptions and our decisions related to risk are complex. They even appear irrational: someone may pass up one risk as unacceptably high, but then and accept another, technically higher, risk without hesitation. This is not necessarily irrational. It may simply be more complicated behavior than we are accounting for. There is an extensive body of literature related to risk perception and acceptability, but here we mainly wish to highlight three issues: risk preference, biased risk perception, and risk communication issues.

**Risk Preference**

Risk preference is simply an individual’s feeling or opinion about risk. Like any preference, risk preference can range from desire to avoidance. In Economics literature, those who desire risks are called “risk-seeking,” while those who avoid risks are called “risk-averse.” Either of these extremes is plausible, and results in behavior which is easy to predict. The trouble is that most people actually seem to exhibit both types of risk preference, as well as anything in-between (which is why real human behavior is difficult to predict).

Such variation is common in financial risk preference. For example, suppose I offer you a chance to play a game: we’ll flip a coin; if it comes up heads I’ll pay you $5, but if it
comes up tails you pay me $1. Would you take the offer? Most people would, and this makes sense mathematically; on average you should come out $2 ahead. Now suppose I offer a second game: heads, I’ll pay you $5000; tails, you pay me $4800. Would you take the offer? For the second game, you should expect to come out $100 ahead, yet not as many people would be willing to play. Rationally, the second offer is 50 times better than the first, yet many people would take the first offer and decline the second (especially if each game is offered one time only). Why?

These people are implicitly taking more information into account. In addition to (or even instead of) the average expected gain, they are considering the prospects of the full gain and loss, how they would feel in either case. Suddenly gaining $5000 would be great, but for many people, suddenly losing almost $5000 would be terrible! They might not be able to pay the rent, etc. Whereas in the first game you risk only $1, which is no big deal. Thus we see that it could be perfectly reasonable for financial risk preference to vary with such factors as the amount of money at stake and whether the risk is a gain or a loss.

Not surprisingly, similar variations are observed in human preferences for many other types of risks. It is common for the public to hail a plane crash killing 200 people as a terrible disaster, while ignoring the fact that thousands die on the highways every week. We now turn to risk perception for some insight into these preferences.

**Biases in Risk Perception**

Research in Psychology has identified many factors that influence risk perception, contributing to apparently illogical or inconsistent behavior such as described above. Two of the most important factors are known as availability and overconfidence.

The *availability* bias is when people believe that events that are easy to imagine or recall occur more frequently, or are more likely to happen, then is actually the case. This is basically because people rely heavily upon their experiences. Since things which they see or hear of often come readily to mind, people also tend to associate frequent occurrence with things that come readily to mind for different reasons. Thus, anything recently seen or heard, or that made a strong impression, may be overestimated in terms of frequency or likelihood. For this reason, people regularly overestimate striking events like tornadoes or plane crashes (see Figure 3.2.4). Unfortunately, this is also reinforced by biased media coverage, with disproportionate emphasis on high-profile events. The flipside of the

---

* (50% chance to win)*(+5) + (50% chance to lose)*(-1) = $2.50 – $0.50 = +$2.00.
† (50% chance to win)*(+5000) + (50% chance to lose)*(-4800) = $2500 – $2400 = $100.
availability bias is that people tend to discount things they haven’t experienced. This explains the common “it won’t happen to me” mindset, and supports the saying “out of sight, out of mind.”

![Figure 3.2.4: Estimated vs. Actual Deaths Per Year (Kahneman et al.)](image)

Overconfidence is when people have undue certainty about the accuracy of something. Repeated experiments have shown that people consistently and seriously underestimate the likelihood that their ideas could be wrong. This bias is also prevalent when people are asked to estimate ranges describing something with a given confidence (e.g., upper and lower bounds such that there is a 98% chance the true answer is within them); the ranges supplied tend to be considerably narrower than the true ranges. Even expert judgment has been found to be highly subject to overconfidence.

The availability and overconfidence biases should not be viewed pejoratively; they are simply properties of human thinking. We have addressed them here to partially explain
“irrational” risk preferences, which in truth may be perfectly reasonable, merely complex. This is important to remember whenever dealing with public opinions about risk.

**Risk Communication Issues**

Possibly the most important aspect of risk management is communication. Many aspects of risk assessment are difficult to convey, especially if the audience has preconceived notions that may be biased or even flat-out incorrect. Yet clear communication is the only remedy. Moreover, a poor job communicating will only reinforce confusion, suspicion, and resistance. For these reasons, it is critical to design presentations and other messages carefully, with attention to the ways they could be received. To conclude, here are a few tips to keep in mind when communicating about risk:

- The way information is presented is important. A 30% increase in mortality rate sounds bad, while annual deaths rising from 1 in a million to 1.3 sounds trivial.
- When arguing that something is safe, emphasize the positives; if it is unsafe, emphasize the negatives. But never distort, mislead, or take out of context.
- Your first statistic (or declarative statement) frames the discussion. The audience will consider any other numbers (or ideas) you present in comparison to it.
- Never dismiss others as wrong or ignorant. Make an effort to understand their views, find similarities in your own views, and then work to resolve differences.