CHAPTER 1

Introduction to Risk Assessment

On any given day, in every corner of the world people are actively working, going to school, driving or taking mass transit to work, relaxing at home or on vacation, or even working at home. Some people are even finding the time to sleep. Those who are working perform jobs that range from cleaning animal kennels to being the head of state of a country and every type of job in between. Every job, in fact, every activity a human performs, has a hazard associated with it. The common hazards we all are exposed to include

- slips, trips, and falls;
- illness and disease;
- food borne illness;
- transportation: car accidents, pedestrian accidents, and bicycle accidents;
- sports: organized sports (football, basketball, soccer) accidents, individual sports accidents (skiing, water sports, skate boarding);
- electrical;
- fires;
- snow removal.
On top of these more common hazards, every job has specific hazards associated with it. The major hazards associated with cleaning animal cages, for example, include

- being attacked by the animal;
- the bacteria, viruses, and parasites that might be in the animal waste;
- the design of the cage might pose problems: size, shape, material of construction, and sharp edges;
- the maintenance of the cage might pose problems: cleanliness, jagged metal or wood, and faulty locks/latches/gates/door;
- the condition of the floor;
- the electrical and/or Heating Ventilation and Air Conditioning (HVAC) system in the building;
- the building’s environmental conditions.

The major hazards associated with being a head of state include

- stress from decision making;
- stress from the potential for war;
- stress from political rivals;
- potential for assassination;
- potential for transportation accidents: airplane crashes (i.e., the President of Poland died in an airplane crash in Russia in 2010 (1).)

Hazardous occupations, for instance, fire fighting, have numerous hazards associated with day-to-day activities. Risk assessment tools and techniques can be used to analyze individual jobs for risks. It is obvious that every activity the President does is analyzed for hazards. Jobs or tasks such as fire fighting, chemical plant worker, electrician, and even office workers are usually analyzed using tools such as job hazard analysis (2).

The focus of this book is on analyzing complex systems, tasks, and combinations of tasks for hazards and the associated risks. Most of the major accidents that occur each year result from a series of events that come together in an accident chain or sequence and result in numerous
deaths, environmental consequences, and property destruction. These accidents can occur anytime in the system’s life cycle. One of the events from history that demonstrates this is the sinking of the Swedish ship Wasa (pronounced Vasa) on August 10, 1628 (3). The ship was fabricated between 1626 and 1628. In those days, engineering of the ships was performed by the shipwright, and he used his experience to determine factors such as center of mass and the amount of ballast the ship should have. Because of various events, pressure was put on the shipbuilders to complete the ship ahead of the planned delivery time. The ship was completed and ready for sail on August 10, 1628. The ship was very ornately decorated and was heavily laden with armament. As the ship left port on its maiden voyage on that calm morning, a gust of wind hit the ship, filling her sails. The ship heeled to port and the sailors cut the sheets. The ship righted itself, but then another gust of wind hit the ship and it tipped to port far enough that water entered the gun ports. This was the event that led to the loss of the ship and approximately 30–50 lives. However, the loss of the ship was probably due to one of the two design flaws. The first factor being that the ship was probably too narrow for its height, and second, the ship did not carry enough ballast for the weight of its guns on the upper decks. A contributing factor was the height above sea level of the gun ports that allowed water to enter the ports when the ship listed to port. Since, as stated above, engineering of ships was more seat of the pants than a systematic design process, the real reason(s) for the disaster can only be speculated. The ship was raised from her watery grave in 1959 and has since been moved to a beautiful museum facility in Stockholm. Therefore, the ship itself can be studied, but other factors such as whether the guns were properly secured, how much provisions were on the ship, and so forth will remain a mystery. The Wasa accident occurred in the ship’s initial phases of its life cycle. Accidents can occur in any phase of a system’s life cycle.

A much more recent accident occurred on December 24, 2008, in Rancho Cordova in which a natural gas leak caused an explosion and fire, killing one person and injuring five others including one firefighter and a utility worker. The explosion also destroyed one house completely and severely damaged two others adjacent to the destroyed house. Several other houses in the neighborhood were damaged. Pacific Gas and Electric Company, the utility owner and operator, operates 42% of California’s natural gas pipe lines.
According to Pacific Gas and Electric Company, the property damage from this explosion and fire was $267,000 (4). The incident involved piping that had been originally installed in 1977 and repaired in 2006. The accident investigators found that a piece of piping that was used in the repair was actually polyethylene pipe used as packing when transporting the ASTM D-2513 grade polyethylene piping. The wall thickness of the packing piping did not meet specifications and there were no print lines of the piping used in the repair. The repair personnel, for whatever reason, selected a piece of the packing piping as the repair material, rather than ensuring the pipe was of the proper grade. Therefore, as with the Wasa event, human error was the primary driver in the event. Although, in both events, hardware components were involved as well.

Risk assessment tools and techniques, if applied systematically and appropriately, can point out these types of vulnerabilities in a system. The key term here is “systematic.” A risk assessment must be systematic in nature to be most effective. A risk assessment should begin early in the life cycle of complex systems. Preliminary hazard analysis (PHA) is an example of a tool that can be applied at the earliest phase of system development. As the design of a system progresses other tools can be applied, such as failure mode and effect analysis (FMEA) and fault tree analysis (FTA). Probabilistic risk assessment (PRA) and human reliability analysis (HRA) are techniques used to analyze very complex systems. These tools usually require a well-developed design, an operating philosophy, and at least working copies of procedures to provide enough material to perform analyses. However, even mature systems benefit from risk assessments. The analyses performed on the space shuttle after the Columbia accident are a good example (5). These assessments pointed out vulnerabilities of the space craft that were previously unidentified or viewed as being not as important.

Using the six sigma/total quality management philosophy of continuous improvement, risk assessment techniques applied throughout the design life of a system can provide insights into safety that might arise at various points of the system’s life cycle (6). Reliability engineers use the bathtub curve to illustrate the classic life cycle of a system (Fig. 1.1) (7). In the first part of a system’s life, there is a higher potential for early failure. The failure rate then decreases to a steady state until some point in the future when systems wear out or old age failure occurs.
Manufacturers usually warranty a system, a car for instance, for the period of time from birth till just before system wear out. This way they maximize their public image, while minimizing their risks or obligations.

Risk analysts are also interested in such curves but from a safety perspective. Accidents commonly occur early in a system’s life cycle because of several reasons, including

- mismatch of materials;
- hardware/software incompatibilities;
- lack of system understanding;
- operator inexperience or lack of training.

The system then enters a long phase of steady-state operation that, as long as no changes perturbate the system, remains safe. In later system life, accidents occur for the same reason as why systems wear out, components wear out. However, in terms of accident risk, when a component fails in old age it might lead to a catastrophic failure of the system, for instance, the Aloha Flight 243 accident (8). In this case, the aircraft structure had become fatigued with age and failed during takeoff. Workers have fewer accidents in their later working years; however, the severity of the injuries may be greater (9). In addition, latent conditions can lay dormant for many years in a system (10). These conditions could be a piece of bad computer code or a
piece of substandard pipe that when challenged leads to a failure. Performing risk assessments on systems throughout their life cycle can help to elucidate these vulnerabilities. Once these vulnerabilities are found, measures can be taken to eliminate them and/or mitigate the consequences of failures. This is the most important step of any risk assessment. That is, eliminating the vulnerabilities and reducing the risk of a system.

1.1 TERMINOLOGY

Risk assessment terminology will be presented throughout the book. However, at this time, several key terms will be defined.

- **Risk**: defined as the probability of an unwanted event that results in negative consequences. Kaplan and Garrick use a set of three questions to define risk (11).
  
  1. What can go wrong?
  2. How likely is it?
  3. What are the consequences?

- **Chapter 2 of this book defines risk in depth.**

- **Probability**: defined as a measure of how likely it is that some event will occur (12).

- **Hazard**: defined as a source of potential damage, harm, or adverse health effects on something or someone under certain conditions at work (13).

- **Severity**: defined as the degree of something undesirable (12).

- **Consequence**: defined as the effect, result, or outcome of something occurring earlier (12).

- **Vulnerability**: defined as a weakness in a system or human that is susceptible to harm (12).

- **Threat**: defined as a source of danger (12). Threat and hazard are considered analogous.

1.2 PERFORMING RISK ASSESSMENTS

There is no absolute rule as to how a risk assessment should be performed and to what depth it should be performed. The NASA
PRA guide (14) provides some recommendations and the Nuclear Regulatory Commission (NRC) provides numerous guideline documents on the topic (15). The Occupational Safety and Health Administration’s (OSHA) “Process Safety Management of Highly Hazardous Chemicals” regulation (29CFR1910.119) (16) requires hazard analyses be performed for certain types of chemical operations, and the Department of Energy (DOE) specifies risk assessments for certain types of facilities (17). However, it is still up to the organization to decide how in depth the analysis should be. This book discusses tools that are effective for performing risk assessments, but the decision as to when to use the tools is up to the risk analyst. Table 1.1 provides a list of the risk assessment tools discussed in this book and at what point in an analysis they are traditionally used. In addition, this book provides other techniques that can be used to enhance a risk assessment, such as task analysis for determining human actions in a process, the Delphi process for eliciting human error probabilities, and the critical incident technique for developing risk scenarios.

### 1.3 RISK ASSESSMENT TEAM

Risk assessment is a systematic, step-by-step approach for evaluating risk. It is the process for determining the probability of a risk occurring and the consequence of that risk. It is a fundamental component of an effective risk management program. This program is a basic management tool consisting of risk assessment and risk control. Risk assessment is the data gathering component, while risk control is the application of the risk assessment evaluation.

#### 1.3.1 Team Approach

Individuals will respond to a risk or perception of a hazard based on their influences, environment, and biases. What one person may perceive as a relatively low risk, another may consider highly dangerous no matter what controls are in place. If one or two individuals are asked to perform an assessment, some relevant factors may be missed or ignored. When determining the best course of action for performing a risk assessment, it is important to remember people will bring their own perceptions. Even in respect to experts, different experts will
## TABLE 1.1
Risk Assessment Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Traditional use</th>
<th>Book chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminary hazard analysis (PHA)</td>
<td>This tool is used in the very beginning of a risk assessment and/or on a conceptual design of a new system, process, or operation. It is used to determine the potential hazards associated with or the potential threats poised to a system, process, or operation. This tool is also useful for organizations to evaluate processes that have been performed for years to determine the hazards associated with them.</td>
<td>5</td>
</tr>
<tr>
<td>Failure mode and effect analysis (FMEA)</td>
<td>This tool is used in system, process, or operations development to determine potential failure modes within the system and provides means to classify the failures by their severity and likelihood. It is usually performed after a PHA and before more detailed analyses.</td>
<td>9</td>
</tr>
<tr>
<td>Failure mode, effects, and criticality analysis (FMECA)</td>
<td>FMECA extends FMEA by including a criticality analysis that is used to chart the probability of failure modes against the severity of their consequences. FMECA can be used instead of an FMEA, in conjunction with an FMEA or after an FMEA has been performed.</td>
<td>10</td>
</tr>
<tr>
<td>Event trees</td>
<td>Event trees are very useful tools to begin to analyze the sequence of events in potential accident sequences. They also have utility in analyzing accidents themselves. Many variations of event trees have been developed. This book presents some of the more common ones.</td>
<td>12</td>
</tr>
</tbody>
</table>
### TABLE 1.1 (Continued)

<table>
<thead>
<tr>
<th>Tool</th>
<th>Traditional use</th>
<th>Book chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault tree analysis (FTA)</td>
<td>FTA is a risk analysis tool that uses Boolean logic to combine events. The lower level events are called <em>basic events</em>, and they are combined with Boolean logic gates into a tree structure, with the undesired event of interest at the top. This event is called the <em>top event</em>. Although this analysis tool is used to quantitatively determine the overall probability of an undesired event, it is also useful from a qualitative perspective to graphically show how these events combine to lead to the undesired event of interest. FTA has a wide range of use from determining how one’s checking account was overdrawn, to determine why a space shuttle crashed.</td>
<td>14</td>
</tr>
<tr>
<td>Human reliability analysis (HRA)</td>
<td>HRA is related to the field of human factors engineering and ergonomics and refers to the reliability of humans in complex operating environments such as aviation, transportation, the military, or medicine. HRA is used to determine the human operators’ contribution to risk in a system.</td>
<td>10</td>
</tr>
<tr>
<td>Probabilistic risk assessment (PRA)</td>
<td>PRA is a systematic and comprehensive methodology to evaluate risks associated with complex engineered systems, processes, or operations such as space craft, airplanes, or nuclear power plant. PRA uses combinations of all the other risk assessment tools and techniques to build an integrated risk model of a system. A fully integrated PRA of a nuclear power plant, for instance, can take years to perform and can cost millions of dollars. It is reserved for the most complex of systems.</td>
<td>15</td>
</tr>
</tbody>
</table>
perceive different risks and from those perceptions, conclude different results or controls. In general, you want to bring together a group of people who work in the environment to work together as a team.

### 1.3.2 Team Representatives

Before any assessment of the risks can be started, a determination of who should be involved or who makes up the risk assessment team needs to be considered. The right group of people with the right mix of experience. The team will be between 5 people up to 10–15, if necessary. The team will include people from all sorts of different jobs and experience.

Risk assessment is never a one man show; it should be conducted by a multidisciplinary team, who has a thorough knowledge of the work to be undertaken. Team members should include management, process or facility engineers, technical personnel, supervisors, production operators, maintenance staff, and safety personnel, if available.

The team members will vary from assessment to assessment, company to company, and industry to industry, but the following elements are common:

1. *Management* should be involved to give practical application in the decision-making process of risk reduction controls and accepting residual risk level.
2. *Engineers* should be involved in the risk assessment process, as they are involved in the development of the design decisions that will impact the overall risk and risk controls.
3. *Workers/Operators/Supervisors* should be involved and included in the team, as these people are the most familiar with the tasks and uses for which the assessment will directly effect. These are the individuals best suited to identify the possible hazards associated with the end use. They can provide valuable insights on the possible controls and the practical application of those controls.
4. *Health and Safety Professionals*, if available, can offer valuable insights into what control measures might be available. They can identify possible hazards and propose risk reduction methods and their application.
5. *Maintenance* is another component that needs to be represented to understand the ramifications of implementing controls on the system or process being assessed.

The goal of the risk assessment team is to reduce risks to tolerable or acceptable levels. This assessment is completed by

1. identifying hazards and/or potential hazards;
2. identifying users and/or tasks;
3. determining the level of risk;
   - low, acceptable
   - medium, moderately acceptable
   - high, not acceptable
4. evaluating potential controls—elimination, substitution, engineering controls, administration controls, and/or use of personal protective equipment;
5. developing a report;
6. implementation and review.

The resulting risk assessment report must be evaluated, approved, and endorsed by senior management.

**REFERENCES**