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 serving as the head of state of a country. 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 and individual sports accidents (skiing, water sports, skate boarding).
- Electrical-related accidents.
- Fires.
- Weather-related accidents.
- Identity theft.
- Internet intrusion.

On top of these more common hazards are specific/major hazards. For example, cleaning animal cages include:

- Being attacked by the animal.
- The bacteria, viruses, and parasites that might be in the animal waste.

Risk Assessment: Tools, Techniques, and Their Applications, Second Edition. Lee T. Ostrom and Cheryl A. Wilhelmsen.

Companion website: www.wiley.com/go/Ostrom/RiskAssessment_2e

- 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 HVAC system in the building.
- The building 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, firefighting, 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 like firefighter, 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 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 10 August 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 the 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 10 August 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 two design flaws: first 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 could 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. The ship itself can be studied, but other factors such as whether the guns were properly secured, how many provisions were on the ship, and so forth will remain a mystery. Accidents can occur in any phase of a system's life cycle. For the Wasa accident, it occurred in the ship's initial phases.

A much more recent accident occurred on 23 February 2018, in Dallas, Texas, in which Atmos Energy, the country's largest natural gas distributor, caused an explosion and fire via a natural gas leak, killing one 12-year-old girl and injuring others (4). Atmos Energy also operates in Colorado, Kansas, Kentucky, Tennessee, Virginia, Louisiana, and Mississippi. The incident involved piping that leaked due to pressure on the piping. The accident investigators found that heavy rain caused underground pressure that pushed rock formations upward, which in turn caused pressure on the system, which caused the leakage. Aging pipes have since been replaced with a more flexible, high-grade plastic. Weather and aging pipes were the primary drivers in the event.

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 and 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 effects 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 program after the Columbia accident are a good example (5). These assessments pointed out vulnerabilities of the spacecraft 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

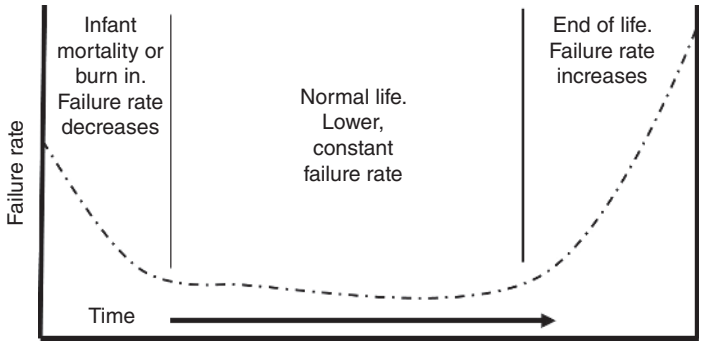

FIGURE 1.1 Bathtub curve.

life cycle (6). Reliability engineers use the bathtub curve to illustrate the classic life cycle of a system (Figure 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 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 wears 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, it 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. In addition, latent conditions can lay dormant for many years in a system (9). These conditions could be a piece of bad computer code or a piece of substandard pipe that when challenged leads to failure. Performing risk assessments on systems throughout their life cycle can help elucidate these vulnerabilities. Once these vulnerabilities are found, measures can be taken to eliminate them and/or measures can be taken to 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 has been defined many ways and for the purposes of this book risk is 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 (10):

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: A measure of how likely it is that some event will occur (11).

Hazard: A source of potential damage, harm or adverse health effects on something or someone under certain conditions at work (12).

Severity: The degree of something undesirable (11).

Consequence: The effect, result, or outcome of something occurring earlier (11).

Vulnerability: A weakness in a system or human that is susceptible to harm (11).

Threat: Source of danger (11). 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 (13) provides some recommendations, and the Nuclear Regulatory Commission (NRC) provides numerous guideline documents on the topic (14). The Occupational Safety and Health Administration's (OSHA) "Process Safety Management of Highly Hazardous Chemicals" regulation (29CFR1910.119) (15) requires that hazard analyses be performed for certain types of chemical operations, and the Department of Energy (DOE) specifies risk assessments for certain types of facilities (16). 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.

TABLE 1.1
Risk Assessment Tools

Tool	Traditional use	Book chapter
Preliminary hazard analysis (PHA)	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	
Failure mode and effects analysis (FMEA)	This tool is used in system, process, or operations development to determine potential failure modes within the system and provides a means to classify the failures by their severity and likelihood. It is usually performed after a PHA and before more detailed analyses	
Failure mode, effects, and criticality analysis (FMECA)	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	
Event trees	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	
Fault tree analysis (FTA)	FTA is a risk analysis tool that uses Boolean logic to combine events. The lower-level events are called basic events, 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 top event. Though 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 over drawn to determining why a space shuttle crashed	

TABLE 1.1
(*Continued*)

Tool	Traditional use	Book chapter
Human reliability analysis (HRA)	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	
Probabilistic risk assessment (PRA)	PRA is a systematic and comprehensive methodology to evaluate risks associated with complex engineered systems, processes, or operations such as spacecraft, 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	

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, which 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 that people will use their own perceptions. Even different experts will perceive different risks and, from those perceptions, conclude different results or controls. In general, bringing together a group of people who work in the environment to work together as a team is ideal.

1.3.2 Team Representatives

Before any assessment of the risks can be started, who should be involved or who makes up the risk assessment team needs to be determined. The team should consist of the right group of people with the right mix of experience. The team will be composed of 5 people, up to 10–15 if necessary, and will include people with different jobs and experiences.

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 they are the most familiar with the tasks and uses for which the assessment will directly affect. 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:
   a. Low: acceptable
   b. Medium: moderately acceptable
   c. 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.

Self-Check Questions

1. How do most of the major accidents occur?
2. What are the following acronyms?
   PHA
   FMEA
   PRA
   HRA
   When should they be applied?
3. What is the goal of a risk assessment team?
4. Who should be involved in the risk assessment team?

REFERENCES

1. CBS (n.d.). Poland's President Killed in Plane Crash. *CBS News*. https://www.cbsnews.com/news/polands-president-killed-in-plane-crash (accessed 4 June 2018).
2. OSHA (n.d.). Job hazard analysis guide. https://www.osha.gov/pls/publications/publication.html (accessed 4 June 2018).
3. Cederlaund, C.O. (2006). *Vasa I, The Archaeology of a Swedish Warship of 1628*. Stockholm: Swedish State Maritime Museum.
4. David, W. (n.d.). Gas service stops for thousands of Dallas homes due to leaks. *The Seattle Times*. https://www.seattletimes.com/nation-world/gas-service-stops-for-thousands-of-dallas-homes-due-to-leaks (accessed 18 June 2018).
5. CAIB (2003). Columbia Accident Investivgation Board, Final Report. NASA.
6. IIARF (n.d.). A global summary of the common body of knowledge 2006. https://na.theiia.org/iiarf/Public%20Documents/2006-CBOK-Summary.pdf (accessed 4 June 2018).
7. Ostrom, L.T. (2018). Bath tub curve diagram.
8. NTSB (n.d.). Aloha Airlines, Flight 243 Boeing 737-200, N73711, Near Maui, Hawaii. https://www.ntsb.gov/investigations/AccidentReports/Reports/AAR8903.pdf (accessed 4 June 2018).
9. Reason, J. (1990). *Human Error*. New York: Cambridge University Press.
10. Kaplan, S. and Garrick, B. (1981). On the quantitive definition of risk. *Risk Analysis* 1 (1): 11–37. https://www.nrc.gov/docs/ML1216/ML12167A133.pdf (accessed 4 March 2019).
11. Farlex (n.d.). The Free Dictionary by Farlex. https://www.the freedictionary.com/severity (19 February 2019).

12. CCOHS (n.d.). Hazards. http://www.ccohs.ca/http://www.ccohs.ca/topics/hazards (accessed 18 June 2018).
13. SMA (n.d.). NASA policy directives. https://sma.nasa.gov/policies/all-policies (accessed 18 June 2018).
14. US NRC (n.d.). NRC regulatory guides: power reactors (Division 1). http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/rg (accessed 18 June 2018).
15. OSHA (n.d.). 1910.119: Process safety management of highly hazardous chemicals. https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.119 (accessed 19 February 2019).
16. DOE (n.d.). Risk Assessment in Support of DOE Nuclear Safety, Risk Information Notice, June 2010. https://www.energy.gov/ea/downloads/risk-assessment-support-doe-nuclear-safety-risk-information-notice-june-2010 (accessed 19 February 2019).