Engineering Ethics

Fourth Edition

Charles B. Fleddermann
University of New Mexico

Prentice Hall
Upper Saddle River • Boston • Columbus • San Francisco • New York • Indianapolis
London • Toronto • Sydney • Singapore • Tokyo • Montreal • Dubai • Madrid
Hong Kong • Mexico City • Munich • Paris • Amsterdam • Cape Town

Vice President and Editorial Director, ECS: *Marcia J. Horton*
Executive Editor: *Holly Stark*
Editorial Assistant: *William Opaluch*
Marketing Manager: *Tim Galligan*
Production Manager: *Pat Brown*
Art Director: *Jayne Conte*
Cover Designer: *Black Horse Designs and Bruce Kenselaar*
Full-Service Project Management/Composition: *Vijayakumar Sekar, TexTech International Pvt Ltd*
Printer/Binder: *Edwards Brothers*
Cover Printer: *Lehigh-Phoenix*

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on appropriate page within text.

Library of Congress Cataloging-in-Publication Data

Fleddermann, Charles B. (Charles Byrns), 1956–
Engineering ethics / Charles B. Fleddermann. — 4th ed.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-13-214521-3 (alk. paper)
ISBN-10: 0-13-214521-9 (alk. paper)
1. Engineering ethics. I. Title.
TA157.F525 2012
174'.962—dc23

2011023371

10 9 8 7 6 5 4 3 2 1

PEARSON

ISBN 10: 0-13-214521-9
ISBN 13: 978-0-13-214521-3

CHAPTER

5 Risk, Safety, and Accidents

Objectives

After reading this chapter, you will be able to

- Know the definitions of risk and safety
- Discover different factors that affect the perception of risk
- Study the nature of accidents
- Know how to ensure that your designs will be as safe as possible.

On a sunny afternoon in May of 1996, Valujet Flight 592 took off from Miami International Airport, heading for Atlanta. Within minutes of leaving the runway, the DC-9's electrical systems started to fail and the cockpit and passenger cabin began filling with smoke. The pilots immediately called the Miami tower for permission to return and began to descend and turn back toward the airport. However, the situation worsened as fire started melting control cables and the pilots became overcome with smoke. The plane suddenly banked sharply and descended rapidly. The descent was so fast that the air-traffic control radar in Miami was no longer able to register an altitude for the airplane. Miraculously, the plane came out of its steep dive and leveled off, either through the efforts of the pilots or because the autopilot came back on. The airplane was now at only 1,000 feet above the ground. The air-traffic controllers in Miami radioed the pilots and attempted to send the aircraft to the closer airport at Opa Locka, Florida. Instead, Flight 592 rolled sharply to the right and, facing nose down, crashed into the Everglades. The two pilots, three flight attendants, and 105 passengers on board were killed.

The subsequent investigation into this accident indicated that the fire was caused by the accidental firing of at least one of many chemical oxygen generators that had been removed from another Valujet airplane and were being carried back to Valujet headquarters in Atlanta. The heat generated by this canister caused a fire in the cargo hold beneath the cockpit that ultimately brought Flight 592 down. The investigation showed that these canisters were improperly secured and shouldn't have been on the airplane at all.

One of the most important duties of an engineer is to ensure the safety of the people who will be affected by the products that he designs. All of the codes of ethics of the professional engineering societies stress the importance of protecting the health and safety of the public in the engineer's duties. As we will see later in this chapter, the cause of the Valujet accident wasn't a flaw in the airplane's design, but rather was attributed to a series of mistakes in handling and securing of the oxygen canisters. What responsibility does the engineer have for ensuring that these types of mistakes are not made? How can products be designed to minimize the risk to the user? We will explore these questions in this chapter.

5.1 INTRODUCTION

No duty of the engineer is more important than her duty to protect the safety and well-being of the public. Indeed, the codes of ethics of the professional engineering societies make it clear that safety is of paramount importance to the engineer. In this chapter, we will look into safety and risk. We will also examine the nature of accidents and try to determine what the engineer's role is in preventing accidents and ensuring the safety of the public.

5.2 SAFETY AND RISK

At the core of many of the cases that we will study are issues of safety and risk. The engineering codes of ethics show that engineers have a responsibility to society to produce products, structures, and processes that are safe. There is an implied warranty with regard to all products that they will perform as advertised—a bridge should allow automobiles to cross from one side of a river to the other, and a computer should correctly perform calculations. Similarly, there is an implied warranty that products are safe to use. Clearly, nothing can be 100% safe, but engineers are required to make their designs as safe as reasonably possible. Thus, safety should be an integral part of any engineering design.

5.2.1 Definitions

Safety is at the same time a very precise and a very vague term. It is vague because, to some extent, safety is a value judgment, but precise because in many cases, we can readily distinguish a safe design from an unsafe one. It is impossible to discuss safety without also including a discussion of risk. Risk is a key element in any engineering design; it is impossible to design anything to be completely risk free. How much risk is appropriate? How safe is safe enough? To answer these questions, we must first study the nature of safety and risk.

The *American Heritage Dictionary* defines risk as the possibility of suffering harm or loss. Risk is sometimes used synonymously with danger. The same dictionary defines safety as freedom from damage, injury, or risk. There is some circularity to these definitions: We engage in risky behavior when we do something that is unsafe, and something is unsafe if it involves substantial risk.

Although these definitions are precise, safety and risk are essentially subjective and depend on many factors:

1. *Voluntary vs. involuntary risk.* Many consider something safer if they knowingly take on the risk, but would find it unsafe if forced to do so. If the property values

are low enough, some people will be tempted to buy a house near a plant that emits low levels of a toxic waste into the air. They are willing to assume the risk for the benefit of cheap housing. However, if a person already living near a plant finds that toxic fumes are emitted by the plant and he wasn't informed, the risk will appear to be larger, since it was not voluntarily assumed. This principle is true even if the level of emission is identical to that in the example of a person choosing to move near the plant.

2. *Short-term vs. long-term consequences.* Something that might cause a short-lived illness or disability seems safer than something that will result in permanent disability. An activity for which there is a risk of getting a fractured leg will appear much less risky than an activity with a risk of a spinal fracture, since a broken leg will be painful and disabling for a few months, but generally full recovery is the norm. Spinal fractures, however, can lead to permanent disability.
3. *Expected probability.* Many might find a one-in-a-million chance of a severe injury to be an acceptable risk, whereas a 50:50 chance of a fairly minor injury might be unacceptable. Swimming at a beach where there is known to be a large concentration of jellyfish would be unacceptable to many, since there would be a high probability of a painful, though rarely fatal, sting. Yet, at the same beach, the risk of a shark attack is low enough that it doesn't deter anyone from swimming, even though such an attack would very likely lead to death or dismemberment. It is important to remember here that the expected probability is only an educated guess.
4. *Reversible effects.* Something will seem less risky if the bad effects are ultimately reversible. This concept is similar to the short-term vs. long-term risk question discussed previously.
5. *Threshold levels for risk.* Something that is risky only at fairly high exposures will seem safer than something with a uniform exposure to risk. For example, the probability of being in an automobile accident is the same regardless of how often you drive. (Of course, you can reduce the likelihood of being in an accident by driving less often.) In contrast, studies have shown that low levels of nuclear radiation actually have beneficial effects on human health, while only at higher levels of exposure are there severe health problems or death. If there is a threshold for the effects, generally there will be a greater tolerance for risk.
6. *Delayed vs. immediate risk.* An activity whose harm is delayed for many years will seem much less risky than something with an immediate effect. For example, for several years now, Americans have been warned about the adverse long-term health effects of a high-fat diet. This type of diet can lead to chronic heart problems or stroke later in life. Yet, many ignore these warnings and are unconcerned about a risk that is so far in the future. These same people might find an activity such as skydiving unacceptably risky, since an accident will cause immediate injury or death.

Thus, whether something is unsafe or risky often depends on who is asked. Something that one person feels is safe may seem very unsafe to someone else. This creates some confusion for the engineer who has to decide whether a project is safe enough to be pursued. In making a decision, some analysis methods, especially line drawing and flow charting, can be used. Ultimately, it is up to the engineer and company management to use their professional judgment to determine whether a project can be safely implemented.

5.2.2 Engineers and Safety

Since safety is an essential aspect of our duties as engineers, how can we be sure that our designs are safe? There are four criteria that must be met to help ensure a safe design.

First, the minimum requirement is that a design must comply with the applicable laws. This requirement should be easy to meet, since legal standards for product safety are generally well known, are published, and are easily accessible.

Second, a design must meet the standard of "accepted engineering practice." You can't create a design that is less safe than what everyone else in the profession understands to be acceptable. For example, federal safety laws might not require that the power supply in a home computer be made inaccessible to the consumer who opens up her computer. However, if most manufacturers have designed their supplies so that no potentially lethal voltages are accessible, then that standard should be followed by all designers, even if doing so increases the cost of the product. A real-life example of this will be shown later when we consider the DC-10 case, in which an airframe was adapted from another design, but was not in accordance with the practice of other aircraft manufacturers at the time. This requirement is harder to comply with than the legal standard, since "accepted engineering practice" is a somewhat vague term. To address this issue, an engineer must continually upgrade her skills by attending conferences and short courses, discussing issues with other engineers, and constantly surveying the literature and trade magazines for information on the current state of the art in the field.

Third, alternative designs that are potentially safer must be explored. This requirement is also difficult to meet, since it requires a fair amount of creativity in seeking alternative solutions. This creativity can involve discussing design strategies with others in your field and brainstorming new alternatives with them. The best way to know if your design is the safest available is to compare it to other potential designs.

Fourth, the engineer must attempt to foresee potential misuses of the product by the consumer and must design to avoid these problems. Again, this requires a fair amount of creativity and research. It is always tempting to think that if someone is stupid enough to misuse your product and is injured, then it's his own fault and the misuse and its consequences shouldn't bother you too much. However, an engineer should execute designs in such a way as to protect even someone who misuses the product. Juries aren't always concerned with the stupidity of the user and might return a substantial judgment against you if they feel that a product was not properly designed. Placing a warning label on a product is not sufficient and is not a substitute for doing the extra engineering work required to produce a safe design.

Finally, once the product is designed, both prototypes and finished devices must be rigorously tested. This testing is not just to determine whether the product meets the specifications. It should also involve testing to see if the product is safe. The importance of adequate testing can be illustrated by the *Kursk* submarine disaster. The *Kursk* was a Russian navy submarine that sank in August of 2000, killing everyone on board. The sinking has been attributed to an explosion in the torpedo room that ripped open a large hole in the hull. Many crew members of the *Kursk* survived the initial explosion, but died because they were unable to escape from the submarine, and no attempts at rescue by other ships were successful. The June 3, 2002, edition of *Time* reported that Russian naval engineers say that the *Kursk* was equipped with a rescue capsule designed to allow crew members to float safely to the surface in an emergency. However, in the rush to get the submarine into service, this safety system was never tested. After the accident, some of the survivors attempted to rescue themselves by using this system, but it did not function properly. It is essential that in any engineering design, all safety systems be tested to ensure that they work as intended.

5.2.3 Designing for Safety

How should safety be incorporated into the engineering design process? Texts on engineering design often include some variation on a basic multistep procedure for effectively executing engineering designs. One version of this process is found in Wilcox [1990] and is summarized as follows:

1. Define the problem. This step includes determining the needs and requirements and often involves determining the constraints.
2. Generate several solutions. Multiple alternative designs are created.
3. Analyze each solution to determine the pros and cons of each. This step involves determining the consequences of each design solution and determining whether it solves the problem.
4. Test the solutions.
5. Select the best solution.
6. Implement the chosen solution.

In step 1, it is appropriate to include issues of safety in the product definition and specification. During steps 2 through 5, engineers typically consider issues of how well the solution meets the specifications, how easy it will be to build, and how costly it will be. Safety and risk should also be criteria considered during each of these steps. Safety is especially important in step 5, where the engineer attempts to assess all of the trade-offs required to obtain a successful final design. In assessing these trade-offs, it is important to remember that safety considerations should be paramount and should have relatively higher weight than other issues.

Minimizing risk is often easier said than done. There are many things that make this a difficult task for the engineer. For example, the design engineer often must deal in uncertainties. Many of the risks can only be expressed as probabilities and often are no more than educated guesses. Sometimes, there are synergistic effects between probabilities, especially in a new and innovative design for which the interaction of risks will be unknown. Risk is also increased by the rapid pace at which engineering designs must be carried out. The prudent approach to minimizing risk in a design is a "go slow" approach, in which care is taken to ensure that all possibilities have been adequately explored and that testing has been sufficiently thorough. However, this approach isn't always possible in the real world.

Are minimizing risks and designing for safety always the more expensive alternatives? Spending a long time engineering a safer product may seem like a very expensive alternative, especially early in the design cycle before the product has been built or is on the market. This, however, is a very short-term view. A more long-term view looks at the possible consequences of not minimizing the risk. There is a great deal of guesswork involved here, but it is clear that any unsafe product on the market ultimately leads to lawsuits that are expensive to defend even if you don't lose and are very costly if you do lose. The prudent and ethical thing to do is to spend as much time and expense as possible up front to engineer the design correctly so as to minimize future risk of injury and subsequent criminal or civil actions against you.

5.2.4 Risk–Benefit Analysis

One method that engineers sometimes use to help analyze risk and to determine whether a project should proceed is called risk–benefit analysis. This technique is similar to cost–benefit analysis. In risk–benefit analysis, the risks and benefits of a project are assigned dollar amounts, and the most favorable ratio between risks and benefits is sought. Cost–benefit analysis is tricky because it is frequently difficult to assign realistic dollar amounts to alternatives. This task is especially difficult in risk–benefit analysis because risks are much harder to quantify and more difficult to put a realistic price tag on. Still, this can be a useful technique if used as part of a broader analysis, but only if used objectively.

In doing a risk–benefit analysis, one must consider who takes the risks and who reaps the benefits. It is important to be sure that those who are taking the risks are also those who are benefiting. This consideration is fundamental to issues of economic justice in our society and can be illustrated by the concept of "environmental racism," which is the placing of hazardous-waste sites, factories with unpleasant or noxious emissions, etc. near the least economically advantaged neighborhoods. This practice is sometimes thought of as racism because in the United States, these types of neighborhoods are generally disproportionately occupied by minority groups. The only ethical way to implement risk–benefit analysis is for the engineer to ensure to the greatest extent possible that the risks as well as the benefits of her design are shared equally in society.

5.3 ACCIDENTS

Now that we have discussed some basic ideas related to safety and risk, it will also be useful to look at ideas on the nature of accidents and see how these ideas bear on our discussion of safety and the engineer's duty to society. There have been numerous studies of accidents and their causes, with attempts to categorize different types of accidents. The goal of this type of work is to understand the nature of accidents and therefore find ways to try to prevent them. Since the engineer's most important job is to protect the safety of the public, the results of this type of research have an impact on the engineering professional.

There are many ways in which accidents can be categorized and studied. One method is to group accidents into three types: procedural, engineered, and systemic [Langewiesche, 1998]. Procedural accidents are perhaps the most common and are the result of someone making a bad choice or not following established procedures. For example, in the airline industry, procedural accidents are frequently labeled as "pilot error." These are accidents caused by the misreading of an important gauge, flying when the weather should have dictated otherwise, or failure to follow regulations and procedures. In the airline industry, this type of error is not restricted to the pilot; it can also be committed by air-traffic controllers and maintenance personnel. Engineers must also guard against procedural problems that can lead to accidents. These problems can include failure to adequately examine drawings before signing off on them, failure to follow design rules, or failure to design according to accepted engineering practice. Procedural accidents are fairly well understood and are amenable to solution through increased training, more supervision, new laws or regulations, or closer scrutiny by regulators.

Engineered accidents are caused by flaws in the design. These are failures of materials, devices that don't perform as expected, or devices that don't perform well under all circumstances encountered. For example, microcracks sometimes develop in turbine blades in aircraft engines. When these cracks become severe enough, the blade can fail and break apart. Sometimes, this has resulted in the penetration of the cabin by metal fragments, causing injury to passengers. Engineered failures should be anticipated in the design stage and should be caught and corrected during testing.

However, it isn't always possible to anticipate every condition that will be encountered, and sometimes testing doesn't occur over the entire range of possible operating conditions. These types of accidents can be understood and alleviated as more knowledge is gained through testing and actual experience in the field.

Systemic accidents are harder to understand and harder to control. They are characteristic of very complex technologies and the complex organizations that are required to operate them. A perfect example of this phenomenon is the airline industry. Modern aircraft are very complicated systems. Running them properly requires the work of many individuals, including baggage handlers, mechanics, flight attendants, pilots, government regulators and inspectors, and air-traffic controllers. At many stages in the operation of an airline, there are chances for mistakes to occur, some with serious consequences. Often, a single, minor mistake isn't significant, but a series of minor mistakes can add up to a disaster. We will see this type of situation later in this chapter when we study the Valujet crash, in which several individuals committed a series of small errors, none of which was significant alone. These small errors came together to cause a major accident.

The airline industry is not the only complex engineered system in our society that is susceptible to systemic accidents. Both modern military systems, especially nuclear weapons, for which complicated detection and communication systems are relied on for control, and nuclear power plants with complicated control and safety systems, have documented failures in the past that can be attributed to this type of systemic problem.

What are the implications of this type of accident for the design engineer? Because it is difficult to take systemic accidents into account during design, especially since there are so many small and seemingly insignificant factors that come into play, it may seem that the engineer bears no responsibility for this type of accident. However, it is important for the engineer to understand the complexity of the systems that he is working on and to attempt to be creative in determining how things can be designed to avert as many mistakes by people using the technology as possible. As designers, engineers are also partially responsible for generating owner's manuals and procedures for the use of the devices they design. Although an engineer has no way of ensuring that the procedures will be followed, it is important that he be thorough and careful in establishing these procedures. In examining the Valujet accident, we will try to see how engineers could have designed some things differently so that the accident might have been averted.

APPLICATION

CASES

Hurricane Katrina

Residents of coastal regions along the east and gulf coasts of the United States have long been familiar with the devastating effects of hurricanes. Rarely does a season go by without a hurricane striking the mainland United States, causing damage, disruption, and loss of lives near the coast as well as far inland where tornadoes spawned by the hurricane can destroy property while torrential rains flood entire communities. Although communities in the United States have plans for handling hurricanes and other natural disasters, Hurricane Katrina presented unique problems that made the normal issues associated with hurricanes even worse.

Like many hurricanes that hit the United States, Katrina started as a tropical depression, forming in the Caribbean on August 23, 2005. Its first landfall was in

KEY TERMS

Procedural, engineered, and systemic accidents

Risk

Safety

REFERENCES

William Langewiesche, "The Lessons of Valujet 592," *The Atlantic Monthly* , March 1998, pp. 81–98.

Alan D. Wilcox, *Engineering Design for Electrical Engineers,* Prentice Hall, Englewood Cliffs, NJ, 1990.

Hurricane Katrina

Louise Story and Robert Farzad, "Hurricane Katrina, the Cost; Insurers Estimate Damage at $9 Billion, Among Costliest U.S. Storms on Record," *New York Times*, August 30, 2005, Section A, p. 12. Also there are numerous articles about this storm in the *New York Times* and other U.S. newspapers on this and subsequent dates.

Joseph B. Treaster and N. R. Kleinfeld, "Hurricane Katrina: The Overview; New Orleans is Inundated as 2 Levees Fail," *New York Times*, August 31, 2005, Section A, p. 1.

Christopher Hallowell, "A Mighty Challenge," Audubon, May–June 2006, p. 34.

Erp Report, "Hurricane Katrina One Year Later," ASCE website, https://www.asce.org/files/pdf/ch9_WhatWeMustDoNext.pdf.

Valujet 592

William Langewiesche, "The Lessons of Valujet 592," *The Atlantic Monthly*, March 1998, pp. 81–98.

Firestone Tires

Numerous articles can be found on this topic in daily newspapers and weekly news magazines, starting in the summer of 2000 and continuing through the spring of 2001. (See, for example, "An Unwieldy Recall," *Time*, September 4, 2000; "Firestone's Tire Crisis," *Time*, August 21, 2000, and "A Nasty Turn for Ford," *Time*, March 15, 2001.)

Kansas City Hyatt Regency Walkway Collapse

Edward O. Pfrang and Richard Marshall, "Collapse of the Kansas City Hyatt Regency Walkways," *Civil Engineering-ASCE,* July 1982, pp. 65–68.

Ford Crown Victoria Police Interceptor

Richard T. DeGeorge, "Ethical Responsibilities of Engineers in Large Organizations: The Pinto Case," *Business and Professional Ethics Journal*, vol. 1, no. 1, Fall 1981, p. 1.

Michelle Bradford, "Police Not Informed of Suggested Repairs Ford Fails to Warn of Cruisers' Gas Tanks." *Arkansas Democrat-Gazette,* July 13, 2002.

Jennifer Dixon, "Fatalities From Rear-Crash Fires Are Higher Than Government Toll." *Detroit Free Press,* December 8, 2003.

Earle Eldridge and David Kiley. "Ford Crown Victoria's Safety Comes Under Scrutiny." *USA Today,* January 28, 2004.

Andy Lenderman, "Police Raise Safety Fears about Ford Crown Vic." *Albuquerque Tribune,* June 21, 2002.

Teton Dam

Phillip M. Boffey, "Teton Dam Verdict: A Foul-up by the Engineers," *Science*, vol. 195, January 21, 1977, pp. 270–272.

DC-10

Paul Eddy, Elaine Potter, and Bruce Page, *Destination Disaster,* New York Times Book Co., New York, 1976.
Peter French, "What Is Hamlet to McDonnell Douglas or McDonnell Douglas to Hamlet: DC-10," *Business and Professional Ethics Journal*, vol. 1, no. 2, 1982, pp. 1–19.
Peter Newhouse, "The Aircraft Industry," *The New Yorker,* June 14, 21, 28 and July 5, 1982.

Cell Phones

New York Times, February 13, 1997, Section A, p. 30.
New York Times, April 25, 1997, Section B, p. 23.
New York Times, June 30, 1997, Section D, p. 9.
Joelle Tessler, "Study: Driver Texting, Phone Bans Ineffective," *Albuquerque Journal*, January 30, 2010, p. A2.

Nanotechnology

Alivisatos, P. "Less is more in medicine: sophisticated forms of nanotechnology will find some of their real-world applications in biomedical research, disease diagnosis, and, possibly, therapy," *Scientific American*, September 2001, p. 186.
Joint Report of The National Academy of Engineering and the Royal Society, "Nanoscience and Nanotechnologies: Opportunities and Uncertainties," available at http://www.nanotec. org.uk/finalReport.htm.
Lam, C. W., James, J. T., Mccluskey, R., Hunter, R. L., "Pulmonary Toxicity of Single-Wall Carbon Nanotubes in Mice 7 and 90 Days After Intratracheal Instillation," *Toxicological Sciences,* January 2004, v. 77, no. 1, pp. 126–134.
Etc Group Comminique, "No Small Matter! Nanotech Particles Penetrate Living Cells and Accumulate in Animal Organs," available at: http://www.etcgroup.org/article.asp?newsid=356.

The Tokaimura Criticality Accident

"Takaimura Criticality Accident", website of the World Nuclear Association, http://www.world-nuclear.org/info/inf37.html.

PROBLEMS

5.1 Think of some type of risky or unsafe behavior in which you have participated. What made it seem unsafe? Why did you do it anyway? What does this tell you about your role as an engineer?

HURRICANE KATRINA

5.2 What responsibility do engineers have for the failure of the levee system in New Orleans after Hurricane Katrina?