CHAPTER SIX

The Engineer's Responsibility to Assess and Manage Risk

Main Ideas in This Chapter

- **Engineers impose risks on the public in design and in management of engineered systems and infrastructure and have an obligation to assess and manage these risks.**
- **Engineers and risk experts define risk as the product of the probability of a harm and the magnitude of that harm.**
- **In quantifying risks, engineers and risk experts have traditionally considered only harms that are relatively easily quantified, such as economic losses, bodily injury, or the number of lives lost.**
- **In a new version of the way engineers and risk experts deal with risk, the "capabilities" approach focuses on the broader effects of risks and disasters on the capabilities of people to live the kinds of lives they value.**
- **The public is concerned about informed consent and the just distribution of risk.**
- **Engineers have techniques for estimating the causes and likelihood of harm, but their effectiveness is limited.**

ON THE FOGGY SATURDAY MORNING of July 28, 1945, a twin-engine U.S. Army Air Corps B-25 bomber lost in the fog crashed into the Empire State Building 914 feet above street level. It tore an 18-by-20-foot hole in the north face of the building and scattered flaming fuel into the building. New York firemen put out the blaze in 40 minutes. The crew members and 10 persons at work perished.[1] The building was repaired and still stands.

Just 10 years later, in 1955, the leaders of the New York City banking and real-estate industries got together to initiate plans for the New York City World Trade Center (WTC), which would later become known as the Twin Towers, the world's tallest buildings at the time.[2] However, as the plans emerged, it became clear that the buildings required new construction techniques.

On September 11, 2001, terrorists attacked the Twin Towers by flying two hijacked Boeing 727 passenger jets into them, each jet smashing approximately two-thirds of the way up its respective tower. A significant consequence of the attack was the fire that started over several floors fed by the spilled jet fuel. The fires isolated

more than 2,000 workers in the floors above them. Only 18 of the more than 2,000 were able to descend the flaming stairwells to safety. Most of the 2,000 perished in the subsequent collapse of the buildings. By comparison, almost all of the workers in the floors below the fire were able to make it down to safety before the towers collapsed. Differences in high-rise building construction techniques as well as the difference in the quantity of fuel involved are factors in the very different performance of these newer structures compared to the Empire State Building.

In the hour following the plane crashes that destroyed or damaged many exterior columns and removed the fire protection from others, the prolonged and intense heat of the flames (more than 1,000 degrees Fahrenheit) caused the structural steel members to lose strength, resulting in beams sagging and an inward deflection of the remaining exterior columns. As a result, the floor structures broke away from the exterior columns. As the top floors fell, they created impact loads on the lower floors that the columns could not support and both buildings progressively collapsed.[3]

For an engineer, 9/11 raises questions of how these structural failures could have happened, why the building codes did not better protect the public, and how to reduce the risk of such disasters in the future. There are even larger questions about acceptable risk and the proper approach to risk as an issue of public policy.

6.1 INTRODUCTION

The concern for safety is ever-present in engineering. How should engineers deal with issues of safety and risk, especially when they involve possible liability for harm? Changes in building technology from the time of the Empire State Building, which withstood the impact and fire caused by the B-25 aircraft, until the time of the design and construction of the World Trade Center, have been hypothesized as factors in the very different performance of the two towers under similar events. The Empire State Building involved much heavier construction with significant masonry cladding compared to the lighter glass cladding of the WTC towers. Most importantly, the steel columns of the Empire State building were protected from fire by an 8 in. thick layer of concrete that also served to carry part of the axial loads and the stairwells were designed to be "fireproof," which allowed most occupants safe egress. The lighter construction techniques in the WTC reduced construction costs for taller buildings and required less massive columns for comparable heights. The lighter columns were certainly an important difference in increasing the vulnerability to both impact and fire damage, compared to the Empire State Building. This illustrates an important fact: engineering necessarily involves risk and risk changes as technology changes. One cannot avoid risk simply by remaining with tried and true designs, but new technologies involve risks that may not be as well understood, potentially increasing the chance of failure or even introducing a previously unknown mode of failure. Without new technology, there is no progress. A bridge or building is constructed with new materials or with a new design. New machines are created and new compounds synthesized, always without full knowledge of their long-term effects on humans or the environment. Even new hazards can be found in products, processes, and chemicals that were once thought to be safe. Thus, risk is inherent and dynamic in engineering.

While engineering and construction practices change gradually over time, engineering practices also change as risks change or as our understanding of risks changes. The International Code Council's (ICC) 2009 edition of the International

Building Code (IBC), which is a model code that is adopted by many jurisdictions, includes several significant changes in rules for design and construction and in fire protection representing lessons learned from the collapse of the World Trade Center buildings. And, these changes happened much faster than the evolutionary changes in building practices and building construction methods which were by comparison gradual between the time of design and construction of the Empire State Building and the World Trade Center buildings.

As noted in Chapter 1, now virtually all engineering codes of ethics give a prominent place to safety, stating that engineers must hold paramount the safety, health, and welfare of the public. The first Fundamental Canon of the National Society of Professional Engineers Code requires members to "hold paramount the safety, health, and welfare of the public." Section III.2.b instructs engineers not to "complete, sign, or seal plans and/or specifications that are not in conformity with applicable engineering standards." Section II.1.a instructs engineers that if their professional judgment is overruled in circumstances that endanger life or property, they shall notify their employer or client and such other authority as may be appropriate. Although "such other authority as may be appropriate" is left undefined, it probably includes those who enforce local building codes and regulatory agencies.

Safety and risk obviously are related ideas; engineers work to make their designs safer. However, no activity or system is perfectly risk free and making any engineered system safer generally means increasing the cost of that system. Engineered systems that are too expensive are not affordable to the taxpaying public or to the purchasing consumer, which means cost constraints are very real. Designing engineers must try to achieve acceptably safe designs that are still affordable and engineers operating engineered systems must work to operate those engineered systems in ways that are acceptably safe, which is to say in ways that do not introduce unacceptable risks. Generally acceptable levels of safety are codified in design codes for the product or system in question and the designing engineer only has to adhere to accepted practice as described in the design codes. However, if the designer develops an innovative design that deviates from accepted practice in some way, the resulting innovative design may introduce previously unidentified risks.

Engineers are concerned with many kinds of risks. Engineers of course face the same risks of everyday living as everyone else, including financial and personal safety, and sometimes there are job site risks or other specific risks to personal safety associated with specific tasks. Many engineers are also businessmen or businesswomen, and in that role they are certainly concerned with the organizational and financial risks associated with running a business. However, in this chapter we focus on the risks imposed on the public by engineering work, which has a role-specific ethical dimension. We will present an engineering definition of risk and look at the different ways that engineering work can affect risks to the public. We will examine how engineers can identify and assess the risks imposed by their work and discuss the moral questions related to determining which risks are acceptable.

6.2 THE ENGINEER'S APPROACH TO RISK

An Engineering Definition of Risk

To assess a risk of harm, an engineer must identify it and quantify it. Engineers often define risk as the product of the probability (p_i) of a harm and the magnitude (h_i) of that

harm as in Equation 6.1. The units of risk defined in this way are the units of the harm being considered, so risks with different harms can't be added or directly compared. The summation notation then implies the summation of all risk components with similar harms. For example, it is possible to estimate the risk of death by electrocution for a utility lineman performing a specific maintenance operation and it is possible to estimate the risk of economic loss resulting from a bridge collapse, but a comparison of these two different calculated risks is not meaningful because they have different harms, and thus units. However, the risk of death in a bridge collapse could be compared with, or added to, the risk of lineman death in power line maintenance operations.

$$Risk = \sum_{i=1}^{n} p_i h_i \tag{6.1}$$

Engineers have traditionally thought of harms in terms of things that can be relatively easily quantified, such as loss of life, personal injury or illness, and damage to property or the environment. Increasingly, engineers are also considering impairment of "capabilities" that allow us to live the kind of life we enjoy. We will discuss this new view of risk in more detail later.

How Engineers Impose and Manage Risks

Risk is imposed, and managed, in different ways in different engineering tasks. Risk is managed in engineering design by design codes—rules proven to produce designs consistent with accepted engineering practice and which do not introduce unacceptable risks. These design rules usually focus on proportioning the system so that the capacity (strength) of the design exceeds the demands (loads) by a specified margin, but design rules sometimes also invoke some basic engineering principles, such as redundancy, the design for failure modes that give visible or audible warnings, or load-limiting devices. For example, highway bridge design rules promulgated by the American Association of State Highway and Transportation Officials (AASHTO) were modified to require more redundancy in a class of fracture-critical highway bridges after the 1967 rush-hour collapse of the Silver Bridge, an eyebar-chain suspension bridge over the Ohio River that resulted in 46 deaths. That failure also triggered more stringent bridge inspection and maintenance requirements for all highway bridges.

Risk is also managed in the operation of engineering systems by development of and adherence to proven operational and maintenance rules. Consider the 1979 crash of American Airlines Flight 191 in Chicago. During takeoff, the left engine and pylon separated from the wing, damaging hydraulic lines and leading to an uncontrolled crash resulting in 273 deaths and loss of the DC-10 aircraft. The failure was caused by unapproved maintenance procedures used to service the spherical bearings connecting the pylon to the wing, which caused cracks in the wing structure. The nonstandard procedure, involving removal of the engine and pylon as a unit, was an innovative effort by several airline maintenance forces because it eliminated the need to disconnect and reconnect many hydraulic, fuel, and electrical lines connecting the engine to the pylon and saved about 200 man-hours per aircraft compared to standardized procedures. But, in the process of removing the engine plus pylon, excess force was applied to mounting points causing cracks in the wing structure.

Operation of a nuclear power plant offers similar but much more complex challenges and with the potential for even greater problems. Continuous training and adherence to standardized processes is critical and frequent review of those processes

is very important. Engineers operating any engineered system should be especially wary about shortcuts and always be watchful for potential weaknesses in the systems they operate. Suppose an operations engineer, thinking broadly about safety, had noticed the vulnerability to tsunami flooding of the backup generators at the Fukushima Nuclear Plant and initiated improvements—perhaps one of the greatest disasters of our time might have been averted.

Sources of Risks Managed by Engineers

The sources of risks that engineers are concerned with include environmental loadings resulting from weather events, seismic events, or even cosmic events, and human actions, both unintentional and intentional. Human error in the design process leading to faulty design of a building can result in collapse with economic losses to the owner, perhaps injury or death for some occupants, and reduction of the tax base for the whole community. Increasingly, engineers are also concerned with attacks on engineered facilities, including both kinetic actions by terrorists and cyberattacks. Assessment of risks resulting from terrorist attack can involve more attributes than probability and harms. Such risk analyses should also include identification of both threats and vulnerabilities, because it can be presumed that in the presence of threats the probability of attack can increase with increasing vulnerability. "Soft" targets are more likely to be attacked while "hardened" facilities and systems can decrease the probability of an attack. In contrast, good seismic engineering does not reduce the probability of an earthquake (although it does reduce the harm of the earthquake). Even without considering the possibility of human error or terrorist attack, good engineering design requires an estimate of the most severe environmental loadings that can reasonably be expected (wind, snow, earthquake, solar storms) and our ability to predict such events is imperfect, which is one reason engineering designs can never be risk free.

Risks are dynamic; actual risks can change during the lifetime of an engineered system. Sometimes this is triggered by the use of new technology—consider the recent observations of dramatically increased seismic activity in areas where hydraulic fracturing is used to stimulate production in shale formations. Whether this will represent a significant new risk to nearby engineered facilities is not yet known. Likewise the risks of storm-induced flooding in coastal areas will increase if sea levels rise. In addition to the dynamic nature of the risk itself, our ability to assess risks and our delineation of acceptable or tolerable risks also change with time. In 2008, the improved understanding of seismic risks and methods to predict tsunami runout compared to the state of knowledge about these risks in the 1960s when the Fukushima Nuclear Plant was designed should have triggered additional risk-management measures at the Fukushima Nuclear Plant. Instead, plant managers did not accept as "realistic" a 2008 internal report suggesting the possibility of much more severe earthquakes and much higher tsunami runouts than the plant designers had considered. Acton and Hibbs[4] highlight the changing understanding of risks in their observation about the Fukushima incident:

> In the final analysis, the Fukushima accident does not reveal a previously unknown fatal flaw associated with nuclear power. Rather, it underscores the importance of periodically reevaluating plant safety in light of dynamic external threats and of evolving best practices….

Risk is generally increased by innovation in both engineering design and in operations. Engineering educators encourage innovative solutions to engineering design

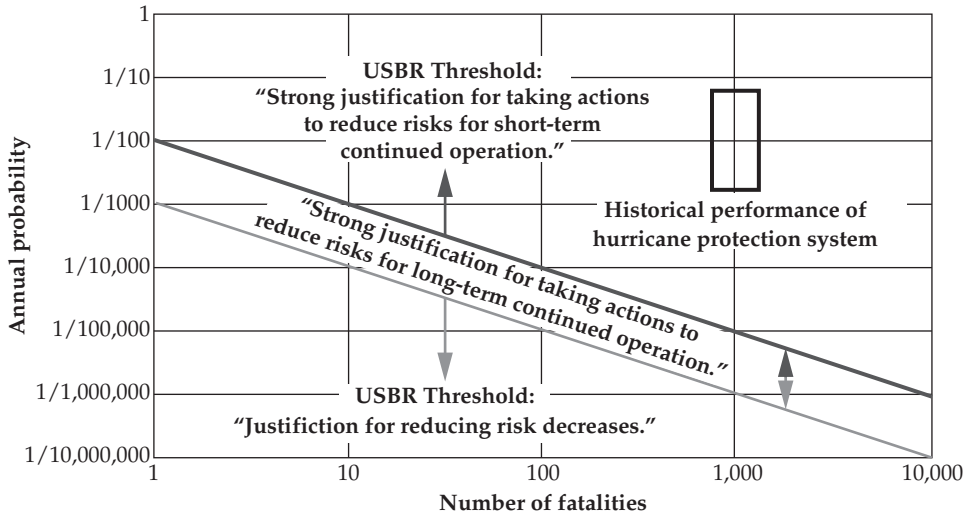
problems, but sometimes fail to emphasize the important relationship between innovation and risk. Innovation, by definition, involves design features or details that are somehow outside the envelope of current practice. Design standards may not anticipate all the issues raised by a particular innovative solution. Thus, many more questions must be addressed by the engineer proposing an innovative solution to make sure newly introduced risks are identified and addressed. The design of the Citicorp building is recognized as a significantly innovative structural engineering solution to an unusual design constraint and the story of that building provides an important illustration of how an engineer is expected to respond when a new risk is identified. But the new risk arose only after the building was placed in service because the structural engineer did not anticipate all the risks introduced by his innovative framing method, which was outside the envelope of standard practice and therefore not anticipated in the design codes. The engineer did not identify and manage this new risk during the design process and we are very fortunate that the risk was even identified before the structure was subjected to design wind loads. In summary, the engineer who chooses to employ truly innovative details or systems has an additional responsibility to identify and address any new risks of failure introduced by the new detail or system. The ability and determination to fulfill this responsibility is an important virtue for an engineer who chooses such innovative solutions in safety-critical designs.

The U.S. Bureau of Reclamation has published recommendations for determining which risk levels justify additional efforts to reduce risks with respect to management of risks caused by dams. These recommendations were discussed in the ASCE's external review[5] of the Katrina flooding as a way to quantify and assess risks associated with the hurricane protection system at New Orleans. The USBR recommendations, presented in Box 6.1, divide the risk of death space (annual probability vs number of fatalities) into three regimes. The lowest risk regime, labeled "Justification for reducing risk decreases" is below an annual risk of death of 10^{-3} (a risk of one death every 1,000 years or 1,000 deaths every 1,000,000 years). The highest risk regime, labeled, "Strong justification for taking actions to reduce risks for short-term continued operation," is above an annual risk of death of 10^{-2}, a risk of one death every 100 years or 1,000 deaths every 100,000 years). Between these two regimes is a regime labeled, "Strong justification for taking actions to reduce risks for long-term continued operation." By comparison, based on its historical performance, the estimated risk of the New Orleans hurricane protection system was well above the higher threshold at a risk of 1,000 deaths every 100 years or an annual risk of death of 10 (one death every 0.1 year). If the USBR recommendations regarding acceptable risk for dams can also be applied to hurricane protection systems, even though they are very different from dams, the risks presented by the pre-Katrina hurricane protection system were unacceptably high and strongly justified additional risk-reducing investment.

One Engineering Approach to Defining Acceptable Risk

The engineering concept of risk focuses on the factual issues of the probability and magnitude of harm and contains no implicit evaluation of whether a risk is morally acceptable. In order to determine whether a risk is acceptable, engineers and risk experts considering engineering solutions often use a cost-benefit analysis that is fundamentally a utilitarian approach. The cost-benefit approach compares the costs,

BOX 6.1 Dam Safety Risk Management Guidelines



Source: U.S. Bureau of Reclamation

including the quantified costs of the imposed risks of the engineering actions under consideration, with the benefits of the actions. Then the engineering solution that maximizes net benefits (benefits minus costs) consistent with economic and other constraints is typically selected. For simplest comparison in a cost-benefit analysis, both the costs and benefits are expressed in equivalent monetary values. This cost-benefit approach to comparing alternative engineering actions has much in common with the utilitarian approach to choices between alternative actions in moral issues. The utilitarian approach to moral issues involves at least a qualitative, if not quantitative, comparison of the utility (benefits) with the harms (costs), allowing the selection of the alternative that results in the greatest good for the greatest number. Given the earlier definition of risk as the product of the probability and the magnitude of harm, we can state the engineer's criterion of acceptable risk in the following way: An acceptable risk is one in which the product of the probability and magnitude of the harm is equaled or exceeded by the product of the probability and magnitude of the benefit.

Consider a case in which a manufacturing process produces bad-smelling fumes that might be a threat to public health. From the cost-benefit standpoint, is the risk to the workers from the fumes acceptable? To determine whether this is an acceptable risk from the cost-benefit perspective, one would have to compare the cost associated with the risk to the cost of preventing or drastically reducing it. To calculate the cost of preventing the harms, we would have to include the costs of modifying the process that produces the fumes, the cost of providing protective masks, the cost of providing better ventilation systems, and the cost of any other safety measures necessary to mitigate the risk. Then we must calculate the cost of not preventing the deaths caused by the fumes. Here, we must include factors such as the cost

of additional health care, the cost of possible lawsuits because of the deaths, the cost of bad publicity, the loss of income to the families of the workers, and other costs associated with the loss of life. If the total cost of preventing the loss of life is greater than the total cost of not preventing the deaths, then the current level of risk is acceptable. If the total cost of not preventing the loss of life is greater than the total cost of preventing the loss, then the current level of risk is unacceptable.

The utilitarian approach to risk embodied in cost-benefit analysis has undoubted advantages in terms of clarity, elegance, and susceptibility to numerical interpretation. Nevertheless, there are several limitations that must be kept in mind.

First, it may not be possible to anticipate all of the effects associated with each option. Insofar as this cannot be done, the cost-benefit method will yield an unreliable result.

Second, it is not always easy to translate all of the risks and benefits into monetary terms. How do we assess the risks associated with a new technology, with eliminating a wetland, or with destruction of habitat important to a particular species of bird in a Brazilian rain forest? Apart from doing this, however, a cost-benefit analysis is incomplete.

The most controversial issue in this regard is, perhaps, the monetary value that should be placed on human life. One way of doing this is to estimate the value of future earnings, but this implies that the lives of retired people and others who do not work commercially, such as housewives, are worthless. So a more reasonable approach is to attempt to estimate a monetary value associated with incremental risks. For example, people often demand a compensating wage to take a job that involves more risk. By calculating the increased risk and the increased pay that people demand for jobs involving greater risk, some economists say, we can derive an estimate of the monetary value people place on such incremental risks to their own lives. Alternatively, we can calculate how much more people would pay to reduce risks in an automobile or other things they use by observing how much more they are willing to pay for a safer car. Unfortunately, there are various problems with this approach. When there are few jobs, a person might be willing to take a risky job he or she would not be willing to take if more jobs were available. Furthermore, wealthy people are probably willing to pay more for increased safety than are poorer people.

Third, cost-benefit analysis in its usual applications makes no allowance for the actual distribution of costs and benefits. Suppose more overall utility could be produced by exposing workers in a plant to a risk of sickness and death. As long as the good of the majority outweighs the costs associated with the suffering and death of those few individual workers who actually are harmed, the risk might be justified by the cost-benefit analysis. Yet, most of us would probably find that an unacceptable account of acceptable risk.

Fourth, the cost-benefit analysis gives no place for informed consent to the risks imposed by technology. We shall see in our discussion of the lay approach to risk that most people think informed consent is one of the most important features of justified risk. As a result, the layperson sometimes disagrees with risk experts (engineers) in assessment of acceptable risks.

The case of the Ford Pinto is an instructive example where the distribution of benefits and harms was grossly inequitable and where the public disagreement about the acceptability of the risk became very obvious. Ford compared the costs and benefits of various upgrades to the fuel tank of the Pinto to reduce the risk of fire

resulting from rear end collisions. Analysis of the risks included assignment of costs for medical treatment of burn victims and a cost of $200,000 for each resulting death. Numbers of accidents, burn victims, and deaths were inferred from the estimated production numbers of the vehicle, vehicle life, and vehicular accident rates. These costs were compared to the costs of an improved fuel tank and filler line system intended to reduce the chance of fuel spills and the cost-benefit calculations favored production of the Pinto without the improvements. While it may seem as if Ford's estimate of the value of human life ($200,000) was far too low, it should be pointed out that in 1970, one of the authors, then a recent engineering graduate with an annual salary of about $10,000, carried only a $5,000 life insurance policy (and drove a Ford Pinto). So it probably was not that particular valuation of human life that so frustrated the juries who heard initial product liability lawsuits and awarded millions to the plaintiffs. Rather, it was probably the fact that being burned alive in an otherwise survivable automobile accident probably ranked high on the jurors' list of unacceptable rights violations and the dramatically unfair distribution of the costs (injuries and deaths to a few unfortunate motorists) compared to the benefits (prices reduced by a few dollars to all purchasers of the Pinto).

Despite these limitations, cost-benefit analysis has a legitimate place in risk evaluation and may be decisive when no serious threats to individual rights are involved. Cost-benefit analysis is systematic, offers a degree of objectivity, and provides a way of comparing risks and benefits by the use of a common measure—namely, monetary cost. But the Pinto case teaches us that an engineer using the utilitarian approach (cost-benefit analysis) to risk assessment in design decisions should always, at the conclusion, consider the equitability of harm and risk distributions and ask him- or herself if a respect-for-persons approach should trump or limit the outcome of the cost-benefit analysis.

Expanding the Engineering Account of Risk: The Capabilities Approach to Identifying Harm and Benefit

As we have pointed out, engineers, in identifying risks and assessing acceptable risk, have traditionally identified harm with factors that are relatively easily quantified, such as economic losses and the number of lives lost.[6] However, four main limitations exist with this rather narrow way of identifying harm. First, often only the immediately apparent or focal consequences of a hazard are included, such as the number of fatalities or the number of homes without electricity. However, hazards can have auxiliary consequences or broader and more indirect harms to society. Second, both natural and engineering hazards might create opportunities, which should be accounted for in the aftermath of a disaster. Focusing solely on the negative impacts and not including these benefits may lead to overestimating the negative societal consequences of a hazard. Third, there remains a need for an accurate, uniform, and consistent metric to quantify the consequences (harms or benefits) from a hazard. For example, there is no satisfactory method for quantifying the nonfatal physical or psychological harms to individuals or the indirect impact of hazards on society. The challenge of quantification is difficult and complex, especially when auxiliary consequences and opportunities are included in the assessment. Fourth, current techniques do not demonstrate the connection between specific harms or losses, such as the loss of one's home and the diminishment of individual or societal well-being and quality of life. Yet, it is surely the larger question of effect on quality of life that is ultimately at issue when considering risk.

In their work on economic development, economist Amartya Sen and philosopher Martha Nussbaum have derived a notion of "capabilities" that the two scholars believe may be the basis of a more adequate way of measuring the harms (and sometimes the benefits) of disasters, including engineering disasters.[7] Philosopher Colleen Murphy and engineer Paolo Gardoni have developed a capabilities-based approach to risk analysis, which focuses on the effect of disasters on overall human well-being. Well-being is defined in terms of individual capabilities or "the ability of people to lead the kind of life they have reason to value." Specific capabilities are defined in terms of functionings or what an individual can do or become in his or her life that is of value. Examples of functionings are being alive, being healthy, and being sheltered. A capability is the real freedom of individuals to achieve a functioning and it refers to the real options he or she has available. Capabilities are constituent elements of individual well-being.

Capabilities are distinct from utilities, which refer to the mental satisfaction, pleasure, or happiness of a particular individual. Often, people's preferences or choices are used to measure satisfaction. Utilities are assigned to represent a preference function. In other words, if an individual chooses A over B, then A has more utility than B. Using utilities to measure the well-being of individuals, however, is problematic because happiness or preference satisfaction is not a sufficient indicator of an individual's well-being. For example, a person with limited resources might learn to take pleasure in small things, which are only minimally satisfying to a person with ample means. The individual in a poverty-stricken situation might have all of his or her severely limited desires satisfied. From the utilitarian standpoint, the person would be described as happy and be said to enjoy a high standard of living. Yet, this individual might still be objectively deprived. The problem here is that utilitarianism does not take into account the number and quality of options that are available to individuals, which is precisely what capabilities capture.

From the capabilities standpoint, a risk is the probability that individuals' capabilities might be reduced due to some hazard. In determining a risk, the first step is to identify the important capabilities that might be damaged by a disaster. Then, to quantify the ways in which the capabilities might be damaged, we must find some "indicators" that are correlated with the capabilities. For example, an indicator of the impairment of the capability for play might be the loss of parks or gym facilities. Next, the indicators must be scaled onto a common metric so that the normalized values of the indicators can be compared. Then, a summary index is constructed by combining the information provided by each normalized indicator, creating a hazard index (HI). Finally, to put the HI into the relevant context, its value is divided by the population affected by the hazard, creating the hazard impact index, which measures the hazard impact per person.

According to its advocates, there are four primary benefits of using the capabilities-based approach in identifying the societal impact of a hazard. First, capabilities capture the adverse effects and opportunities of hazards beyond the consequences traditionally considered. Second, since capabilities are constitutive aspects of individual well-being, this approach focuses our attention on what should be our primary concern in assessing the societal impact of a hazard. Third, the capabilities-based approach offers a more accurate way to measure the actual impact of a hazard on individuals' well-being. Fourth, rather than considering diverse consequences, which increase the difficulty of quantification, the capabilities-based approach requires considering a few properly selected capabilities.[8]

In addition to identifying more accurately and completely the impact of a hazard, its advocates believe the capabilities-based approach provides a principled foundation for judging the acceptability and tolerability of risks.[9] Judgments of the acceptability of risks are made in terms of the impact of potential hazards on the capabilities of individuals. Thus, according to the capabilities approach, a risk is acceptable if the probability is sufficiently small that the adverse effect of a hazard will fall below a threshold of the minimum level of capabilities attainment that is acceptable in principle. The "in principle" qualification captures the idea that, ideally, we do not want individuals to fall below a certain level. We might not be able to ensure this, however, especially immediately after a devastating disaster. In practice, then, it can be tolerable for individuals to temporarily fall below the acceptable threshold after a disaster, as long as this situation is reversible and temporary and the probability that capabilities will fall below a tolerability threshold is sufficiently small. Capabilities can be a little lower, temporarily, as long as no permanent damage is caused and people do not fall below an absolute minimum.

6.3 DIFFICULTIES IN DETERMINING THE CAUSES AND LIKELIHOOD OF HARM: THE CRITICAL ATTITUDE

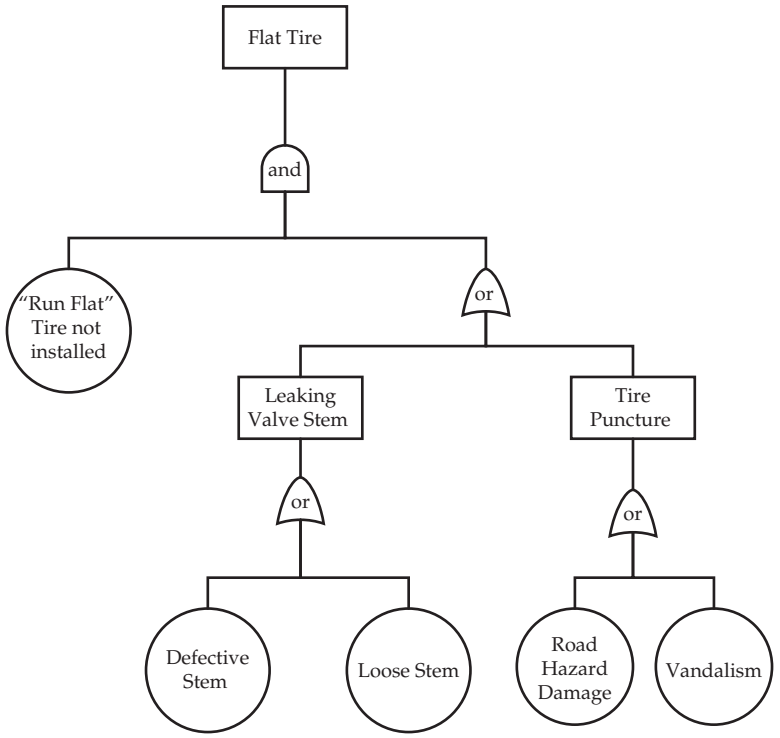
Estimating risk, no doubt defined as estimating the probabilities and magnitudes of some harms, has been described by one writer as looking "through a glass darkly."[10] It would be highly desirable, of course, to be able to accurately predict both the possible harms and the probability of each harm resulting from engineering work. Instead, engineers can only estimate probability and magnitude of any anticipated harm. To make matters worse, often engineers cannot even make estimates satisfactorily. In actual practice, therefore, estimating risk (or "risk assessment") involves an educated guess at the possible undesirable consequences and an uncertain prediction of the probability of each consequence. In this section, we consider some of the methods of estimating risk, the uncertainties in these methods, and the value judgments that these uncertainties necessitate.

Limitations in Identifying Failure Modes

With respect to new technologies, engineers and scientists must have some way of estimating the risks that they impose on those affected by them. One of the methods for assessing risk involves the use of a fault tree analysis (FTA), a formal backward looking deductive analysis, to determine the immediate and basic causes of some undesirable event. In a fault tree analysis, for each identified undesirable event (consequence), Boolean logic is used to identify first the immediate causes of that event and then the basic causes. A probabilistic risk assessment (PRA) can then be conducted to estimate the probabilities of each basic and immediate cause, allowing an estimation of the probability of the event with improved confidence.

Fault trees such as the example illustrated in Box 6.2 are often used to anticipate hazards for which there is little or no direct experience, such as nuclear meltdowns. They enable an engineer to analyze systematically different events or failure modes that could produce the undesirable end result. A failure mode is a way in which a structure, mechanism, system, or process can malfunction. For example, a structural member can fail in tension, crush or buckle in compression, crack or rupture in bending, suffer loss of section and strength because of corrosion or abrasion, burst

BOX 6.2 Fault Tree Example



Fault Tree Analysis of flat tire: A flat tire on your new car can have several causes. If "Run Flat" tires are installed as intended by the manufacturer, then the problem is prevented. But if ordinary tires are instead installed, they can leak at any punctures or through the valve stem. Those two intermediate causes each show two fundamental causes. If probabilities are estimated for the likelihood of each of the basic causes, the probability of a flat tire can be estimated and the risk assessed. If the risk is deemed excessive, the probabilities of some of the basic causes might be reduced by more frequent inspection and/or maintenance or by improved security (parking in a secure garage to reduce the probability of vandalism).

because of excessive internal pressure, or lose strength or even burn because of excessive temperature.

Fault tree analysis has been criticized as offering too optimistic a perspective, most significantly because the fault tree analysis is the estimation of the aggregate probability of identified failure modes. It is sometimes the case that failure modes causing harm are not identified during these analyses. As a result, their risks are not estimated. In such a case, the analysis can be misleading, implying a lower risk than actually exists.

The March 2011 failure and meltdown of the reactors at the Fukushima Nuclear Power Plant is a case in point. The disaster was caused by a tsunami closely following a significant earthquake. The reactors shut down automatically following the earthquake, according to the usual protocol, but the consequent tsunami destroyed the backup electrical generators providing power for the emergency cooling systems. The subsequent delay in providing power to the emergency cooling systems led to meltdowns in three

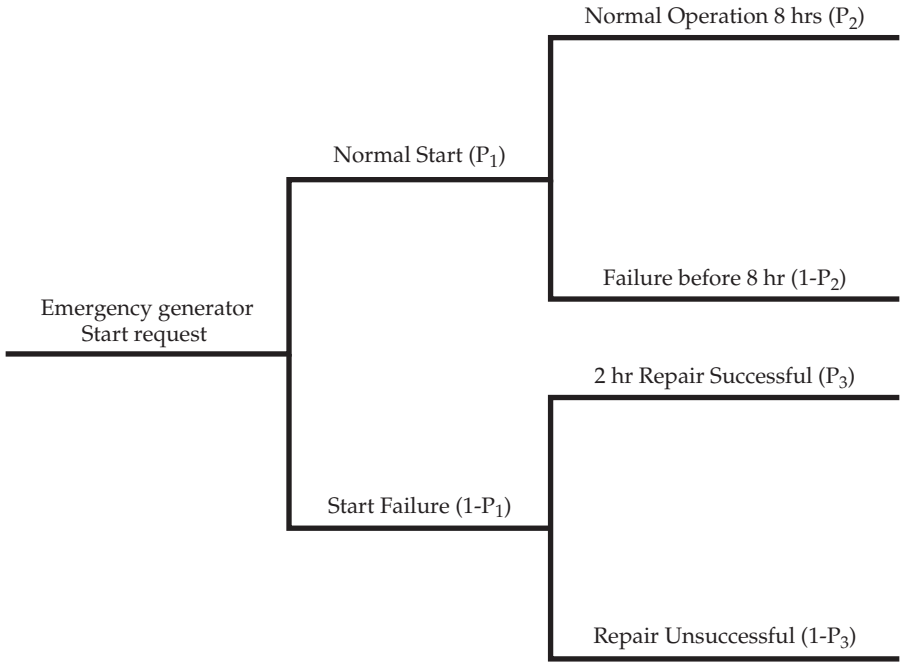
reactors. This failure highlights the need for continued reassessment of design standards for operational plants. According to the World Nuclear Association,

> The tsunami countermeasures taken when Fukushima Daiichi was designed and sited in the 1960s were considered acceptable in relation to the scientific knowledge then, with low recorded run-up heights for that particular coastline. But through to the 2011 disaster, new scientific knowledge emerged about the likelihood of a large earthquake and resulting major tsunami. However, this did not lead to any major action by either the plant operator, TEPCO, or government regulators, notably the Nuclear & Industrial Safety Agency (NISA). The tsunami countermeasures could also have been reviewed in accordance with IAEA [International Atomic Energy Agency] guidelines which required taking into account high tsunami levels, but NISA continued to allow the Fukushima plant to operate without sufficient countermeasures, despite clear warnings.[11]

A different approach to a systematic examination of failure modes is event tree analysis (ETA), a forward looking, inductive approach as illustrated in Box 6.3. In ETA, we reason forward from a hypothetical initiating event to determine what consequences that initiating event might have and then estimate the probabilities of these consequences.

Although engineers rightly believe that it is necessary to go through such analyses to ensure that they have taken into account as many failure modes as possible, the analyses

BOX 6.3 Event Tree Analysis Example



Event Tree Analysis of Emergency Power Failure: This analysis facilitates an estimation of the probability that emergency power supply will not be available for the duration of an 8 hour demand. If the resulting risk of loss of emergency power failure is unacceptable, the risk can be reduced by increasing P_1 (perhaps by increased inspection and preventive maintenance or by adding redundant systems) or by increasing P_3 (perhaps by improved training of maintenance forces or stockpiling of additional repair parts).

have severe limitations. First, it is not possible to anticipate all of the mechanical, physical, electrical, and chemical problems that might lead to failure. For example, the possibility of terrorist attacks has added a new dimension to risk analysis and estimation.

Second, it is never possible to anticipate all of the types of human error that could lead to failure. Third, the probabilities assigned to the failure modes are often highly conjectural and not always based on solid experimental testing. We are not, for example, going to melt down a nuclear reactor to determine the probability of such an occurrence leading to a chain reaction fission explosion. In many cases, we do not know the probability of the behavior of materials at extremely elevated temperatures.

Limitations due to Tight Coupling and Complex Interactions

Sociologist Charles Perrow[12] confirms some of these problems by arguing that there are two characteristics of high-risk technologies that make them especially susceptible to accidents and allow us to speak of "normal accidents." These two features are the "tight coupling" and "complex interactions" of the parts of a technological system. These two factors make accidents not only more likely but also more difficult to predict and control. This, in turn, makes risk more difficult to estimate.

In tight coupling, the temporal element is crucial. Processes are tightly coupled if they are connected in such a way that one process is known to affect another and will usually do so within a short time. In tight coupling, there is usually little time to correct a failure and little likelihood of confining a failure to one part of the system. As a result, the whole system is damaged. A chemical plant is tightly coupled because a failure in one part of the plant can quickly affect other parts of the plant. A university, by contrast, is loosely coupled because if one department ceases to function, then the operation of the whole university is usually not threatened.

In complex interaction, the inability to predict consequences is crucial. Processes can be complexly interactive in that the parts of the system can interact in unanticipated ways. No one dreamed that when X failed, it would affect Y. Chemical plants are complexly interactive in that parts affect one another in feedback patterns that cannot always be anticipated. A post office, by contrast, is not so complexly interactive. The parts of the system are related to one another for the most part in a linear way that is well understood and the parts do not usually interact in unanticipated ways that cause the post office to cease functioning. If a post office ceases to function, it is usually because of a well-understood failure.

Examples of complexly interactive and tightly coupled technical systems include not only chemical plants but also nuclear power plants, electric power grid networks, space missions, and nuclear weapons systems. Being tightly coupled and complexly interactive, they can have unanticipated failures and there is little time to correct the problems or keep them from affecting the entire system. This makes accidents difficult to predict and disasters difficult to avoid once a malfunction appears.

Unfortunately, it is difficult to change tightly coupled and complexly interactive systems to make accidents less likely or even easier to predict. To reduce complexity, decentralization is required to give operators the ability to react independently and creatively to unanticipated events. To deal with tight coupling, however, centralization is required. To avoid failures, operators need to have command of the total system and to be able to follow orders quickly and without question. It may not be possible, furthermore, to make a system both loosely coupled and noncomplex. Engineers know that they can sometimes overcome this dilemma by including

localized and autonomous automatic controls to protect against failures due to complexity and couple them with manual overrides to protect against tight coupling failures. Nevertheless, according to Perrow, some accidents in complex, tightly coupled systems are probably inevitable and, in this sense, "normal."

The following is an example of an accident in a system that was complexly interactive and tightly coupled. In the summer of 1962, the New York Telephone Company completed heating system additions to a new accounting building in Yonkers, New York. The three-story, square-block building was a paradigm of safe design, using the latest technology.

In October 1962, after the building was occupied and the workers were in place, final adjustments were being made on the building's new, expanded heating system located in the basement. This system consisted of three side-by-side, oil-fired boilers. The boilers were designed for low pressures of less than 6.0 psi and so were not covered by the boiler and pressure vessel codes of the American Society of Mechanical Engineers. Each boiler was equipped with a spring-loaded safety relief valve that had been designed to open and release steam into the atmosphere if the boiler pressure got too high. Each boiler was also equipped with a pressure-actuated cutoff valve that would cut off oil flow to the boiler burners in the event of excessive boiler pressure. The steam pressure from the boilers was delivered to steam radiators, each of which had its own local relief valve. Finally, in the event that all else failed, a 1-foot-diameter pressure gauge with a red "Danger Zone" marked on the scale and painted on the face sat on the top of each boiler. If the pressure got too high, the gauge was supposed to alert a custodian who operated the boilers so he could turn off the burners.

On October 2, 1962, the following events transpired:[13]

1. The building custodian decided to fire up boiler 1 in the heating system for the first time that fall. The electricians had just wired the control system for the new companion boiler (boiler 3) and successfully tested the electrical signal flows.
2. The custodian did not know that the electricians had left the fuel cutoff control system disconnected. The electricians had disconnected the system because they were planning to do additional work on boiler 3 the following week. They intended to wire the fuel cutoffs for the three boilers in series (i.e., high pressure in any one would stop all of them).
3. The custodian mechanically closed the header valve because it was a warm Indian summer day and he did not want to send steam into the radiators on the floors above. Thus, the boiler was delivering steam pressure against a blocked valve and the individual steam radiator valves were out of the control loop.
4. As subsequent testing showed, the relief valve had rusted shut after some tests the previous spring in which the boilers had last been fired. (Later, laws were enacted in New York State that require relief valves for low-pressure boiler systems to be operated by hand once every 24 hours to ensure that they are not rusted shut. At the time, low-pressure boiler systems were not subject to this requirement.)
5. This was on Thursday, the day before payday, and the custodian made a short walk to his bank at lunch hour to cash a check soon after turning on boiler 1.
6. The cafeteria was on the other side of the wall against which the boiler end abutted. Employees were in line against the wall awaiting their turn at the cafeteria serving tables. There were more people in line than there would have been

on Friday because on payday many workers went out to cash their paychecks and eat their lunches at local restaurants.

7. Boiler 1 exploded. The end of the boiler that was the most removed from the wall next to the cafeteria blew off, turning the boiler into a rocket-like projectile. The boiler lifted off its stanchions and crashed into the cafeteria, after which it continued to rise at great velocity through all three stories of the building. Twenty-five people were killed and almost 100 seriously injured.

The events that led to this disaster were complexly interrelated. There is no possible way that fault tree or event tree analyses could have predicted this chain of events. If the outside temperature had been cooler, the custodian would not have closed the header valve and the individual steam radiator valves in each upstairs room would have opened. If the relief valve had been hand operated every day, its malfunction would have been discovered and probably corrected. If the time had not been noon and the day before payday, the custodian might have stayed in the basement and seen the high-pressure reading and turned off the burners. If it had not been lunch time, the unfortunate victims would not have been in the cafeteria line on the other side of the wall from the boiler.

The events were also tightly coupled. There was not much time to correct the problem once the pressure started to rise and there was no way to isolate the boiler failure from a catastrophe in the rest of the building. There was one engineering design change that, if adopted, could have broken the chain of events and prevented the accident. It would have been a simple matter to include a fuel flow cutoff if the fuel cutoff system were in any way disabled. However, in complex interconnected systems such as this one, hindsight is always easier than foresight.

Normalizing Deviance and Self-Deception

Still another factor that increases risk and also decreases our ability to anticipate harm is increasing the allowable deviations from proper standards of safety and acceptable risk. Sociologist Diane Vaughn refers to this phenomenon as the "normalization of deviance."[14]

Every design carries with it certain predictions about how the designed object should perform in use. Sometimes these predictions are not fulfilled, producing what are commonly referred to as anomalies. Rather than correcting the design or the operating conditions that led to anomalies, engineers or managers too often do something less desirable. They may simply accept the anomaly or even increase the boundaries of acceptable risk. Sometimes this process can lead to disaster.

This process is dramatically and tragically illustrated by the events that led to the *Challenger* disaster.[15] Neither the contractor, Morton Thiokol, nor NASA expected the rubber O-rings that sealed the joints in the solid rocket booster (SRB) to be touched by the hot gases of motor ignition, much less to be partially burned. However, because previous shuttle flights showed damage to the sealing rings, the reaction by both NASA and Thiokol was to accept the anomalies without attempting to remedy the problems that caused the anomalies.

The following are examples of how deviance was normalized before the disaster:

1. In 1977, test results showed that the SRB joints would rotate open at ignition, creating a larger gap between the tang and clevis. According to NASA engineers, the

gap was large enough to prevent the secondary seal from sealing if the primary O-ring failed late in the ignition cycle. Nevertheless, after some modifications, such as adding sealing putty behind the O-rings, the joint was officially certified as an acceptable risk, even though the joint's behavior deviated from design predictions.[16]

2. Another anomaly was discovered in November 1981 after flight STS-2, which showed "impingement erosion" of the primary O-ring in the right SRB's aft field joint.[17] The hot propellant gases had moved through the "blow holes" in the zinc chromate putty in the joints. The blow holes were caused by entrapped air introduced at the time the putty was installed. Even though this troubling phenomenon was not predicted, the joints were again certified as an acceptable risk.
3. A third anomaly occurred in 1984 with the launch of STS-41-B when, for the first time, two primary O-rings on two different joints were eroded.[18] Again, the erosion on two joints was termed an acceptable risk.[19]
4. Another anomaly occurred in 1985 when "blow-by" of hot gases had reached the secondary seal on a nozzle joint. The nozzle joints were considered safe because, unlike the field joints, they contained a different and quite safe secondary "face seal." The problem was that a similar malfunction could happen with the field joint with the danger much more serious and these problems were not dealt with.
5. Perhaps the most dramatic example of expanding the boundaries of acceptable risk was in the area of the acceptable temperature for launch. Before the *Challenger* launch, the lowest temperature of the seals at launch time was 53 degrees Fahrenheit. (At that time, the ambient temperature was in the high 60s.) On the night before the launch of the *Challenger*, however, the temperature of the seals was expected to be 29 degrees and its ambient temperature below freezing. Thus, the boundaries for acceptable risk were expanded by 24 degrees.

The result of (1) accepting these anomalies without making any adequate attempt to remedy the basic problem (poor seal design) and (2) lowering the temperature considered acceptable for launch was the tragic destruction of the *Challenger* and the loss of its crew. Vaughn argues that these kinds of problems cannot be eliminated from technological systems and that, as a result, accidents are inevitable. Whether or not this is the case, there is no question that technology imposes risk on the public and that these risks are often difficult to detect and eliminate.

The case also illustrates how the self-deception involved in normalizing deviance can limit the ability of engineers to correctly anticipate risk. Some of the engineers, and especially engineering managers, repeatedly convinced themselves that allowing still one more deviation from design expectations would not increase the chance of failure or was at least an acceptable risk. The result was a tragic disaster.

6.4 THE PUBLIC'S APPROACH TO RISK

Expert and Layperson: Differences in Factual Beliefs

Engineers and other experts on risk often believe that the public is confused about risk, sometimes because the public does not have the correct factual information about the likelihood of certain harms. A 1992 National Public Radio story on the

Environmental Protection Agency (EPA) began with a quote from EPA official Linda Fisher that illustrated the risk expert's criticism of public understanding of risk:

> A lot of our priorities are set by public opinion, and the public quite often is more worried about things that they perceive to cause greater risks than things that really cause risks. Our priorities often times are set through Congress … and those [decisions] may or may not reflect real risk. They may reflect people's opinions of risk or the Congressmen's opinions of risk.[20]

Fisher believes that whereas both members of the U.S. Congress and ordinary laypeople may be confused about risk, the experts know what it is. Risk is something that can be objectively measured—namely, the product of the likelihood and magnitude of harm.

The profound differences between the engineering and public approach to risk have been the sources of miscommunication and even acrimony. Two questions then arise: Why does an engineer need to understand these differences? And what are the grounds for these profound differences in outlook on risk?

With respect to the first question, the answer is that the engineer, when quantifying risks and benefits, must remember to think about the public's understanding and acceptance of the risks that the engineer's work will impose and know that it may be very different from the way engineers assess risks. If the engineer makes decisions about the acceptability of a certain risk and somehow miscalculates the public's perception, and if harms should occur from risks considered acceptable in an engineering assessment, the public may view the engineer's actions from a different perspective and unsympathetically. The public, we should remember, sometimes is manifested in groups of 12 serving as juries and charged with evaluating whether engineers have made these decisions about risk in an acceptable manner.

With respect to the second question, the first difference is that engineers and risk experts believe that the public is sometimes mistaken in estimating the probability of death and injury from various activities or technologies. Recall EPA official Linda Fisher's reference to "real risk," by which she meant the actual calculations of probability of harm. Risk expert Chauncey Starr has a similarly low opinion of the public's knowledge of probabilities of harm. He notes that people tend to overestimate the likelihood of low-probability risks associated with causes of death and to underestimate the likelihood of high-probability risks associated with causes of death. The latter tendency can lead to overconfident biasing or *anchoring*. In anchoring, an original estimate of risk is made—an estimate that may be substantially erroneous. See Box 6.4 for important factors in assessing risk acceptability. Even though the estimate is corrected, it

BOX 6.4 Important Factors in Assessing Risk Acceptability

- Laymen have a very different perspective and assessment than risk experts.
- New or unfamiliar risks are more likely to be unacceptable to the public than familiar risks.
- Voluntarily assumed risks are more likely to be considered acceptable than involuntarily imposed risks.
- Jobs involving higher risks generally demand higher wages.
- Free and informed consent, equity, and justice are important factors in acceptability of risk.

is not sufficiently modified from the original estimate. The original estimate anchors all future estimates and precludes sufficient adjustment in the face of new evidence.[21]

Other scholars have reported similar findings. A study by Slovic, Fischhoff, and Lichtenstein shows that although even experts can be mistaken in their estimations of various risks, they are not as seriously mistaken as laypeople.[22] The study contrasts actual versus perceived deaths per year.[23] Experts and laypeople were asked their perception of the number of deaths per year for such activities as smoking, driving a car, driving a motorcycle, riding in a train, skiing, and so on. On a graph that plots perceived deaths (on the vertical axis) against actual deaths (on the horizontal axis) for each of several different risks, if the perception (by either laypeople or experts) of deaths were accurate, then the result would be a 45-degree line. In other words, actual and perceived deaths would be the same for the plots of the perceptions of either laypersons or experts. Instead, the experts were consistently approximately one order of magnitude (i.e., approximately 10 times) low in their perceptions of the perceived risk and the lay public was still another order of magnitude (i.e., approximately 100 times) too low, resulting in lines of less than 45 degrees for experts and even less for laypersons.

"Risky" Situations and Acceptable Risk

It does appear to be true that the engineer and risk expert, on the one hand, and the public, on the other hand, differ regarding the probabilities of certain events. The major difference, however, is in the conception of risk itself and in beliefs about acceptable risk. One of the differences here is that the public often combines the concepts of risk and acceptable risk—concepts that engineers and risk experts separate sharply. Furthermore, public discussion is probably more likely to use the adjective "risky" than the noun "risk."

We can begin with the concepts of "risk" and "risky." In public discussion, the use of the term "risky," rather than referring to the probability of certain events, more often than not has the function of a warning sign, a signal that special care should be taken in a certain area.[24] One reason for classifying something as risky is that it is new and unfamiliar. For example, the public may think of the risk of food poisoning from microbes as being relatively low, whereas eating irradiated food is "risky." In fact, in terms of probability of harm, there may be more danger from microbes than radiation, but the dangers posed by microbes are familiar and commonplace, whereas the dangers from irradiated foods are unfamiliar and new. Another reason for classifying something as risky is that the information about it might come from a questionable source. We might say that buying a car from a trusted friend who testifies that the car is in good shape is not risky, whereas buying a car from a used car salesman whom we do not know is risky.

Laypeople do not evaluate risk strictly in terms of expected deaths or injury. They consider other factors as well. For example, they are generally willing to take voluntary risks that are 1,000 times (three orders of magnitude) as uncertain as involuntary risks. Thus, voluntarily assumed risks are more acceptable than risks not voluntarily assumed. The amount of risk people are willing to accept in the workplace is generally proportional to the cube of the increase in the wages offered in compensation for the additional risk. For example, doubling wages would tend to convince a worker to take eight times the risk. But laypeople may also separate by three orders of magnitude the risk perceived to be involved in involuntary exposure

to danger (e.g., when a corporation places a toxic waste dump next door to one's house) and the risk involved in voluntary exposure (e.g., smoking). Here, voluntarily assumed risks are viewed as inherently less risky, not simply more acceptable. Laypeople also seem to be content with spending different amounts of money in different areas to save a life. In his study of 57 risk-abatement programs at five different government agencies in Washington, DC, including the EPA and the Occupational Safety and Health Administration (OSHA), Starr shows that such programs vary greatly in the amount of money they spend to save a life. Some programs spend $170,000 per life, whereas others spend $3 million per life.[25]

Another researcher, D. Litai, has separated risk into 26 risk factors, each having a dichotomous scale associated with it.[26] For example, a risk may have a natural or a human origin. If the risk has a human origin, Litai concludes from an analysis of statistical data from insurance companies that the perceived risk is 20 times greater than a risk with a natural origin. An involuntarily assumed risk, whether of natural or human origin, is perceived as being 100 times greater than a voluntarily assumed risk. An immediate risk is perceived as being 30 times greater than an ordinary one. By contrast, a regular risk is perceived as being just as great as an occasional one and necessary risk is just as great as a luxury-induced one. Here again, there is evidence of the amalgamation of the concepts of risk and acceptable risk.

Two issues in the public's conception of risk and acceptable risk have special moral importance: free and informed consent and equity or justice. These two concepts follow more closely the ethics of respect for persons than utilitarianism. According to this ethical perspective, as we have seen, it is wrong to deny the moral agency of individuals. Moral agents are beings capable of formulating and pursuing purposes of their own. We deny the moral agency of individuals when we deny their ability to formulate and pursue their own goals or when we treat them in an inequitable manner with respect to other moral agents. Let us examine each of these concepts in more detail.

Free and Informed Consent

To give free and informed consent to the risks imposed by technology, three things are necessary. First, a person must not be coerced. Second, a person must have the relevant information. Third, a person must be rational and competent enough to evaluate the information. Unfortunately, determining when meaningful and informed consent has been given is not always easy, for several reasons.

First, it is difficult to know when consent is free. Have workers given their free consent when they continue to work at a plant with known safety hazards? Perhaps they have no alternative form of employment.

Second, people are often not adequately informed of dangers or do not evaluate them correctly. As we have seen, sometimes laypeople err in estimating risk. They underestimate the probability of events that have not occurred before or that do not get their attention, whereas they overestimate the probability of events that are dramatic or catastrophic.

Third, it is often not possible to obtain meaningful informed consent from individuals who are subject to risks from technology. How would a plant manager obtain consent from local residents for his plant to emit a substance into the atmosphere that causes mild respiratory problems in a small percentage of the population? Is the fact that the residents do not protest sufficient evidence that they have consented?

What if they do not know about the substance, do not know what it does, do not understand its effects correctly, or are simply too distracted by other things?

In light of the problems in getting free and informed consent, we could compensate individuals after the fact for actual harms done to them through technology. For example, people could be compensated for harms resulting from a defective design in an automobile or a release of a poisonous gas from a chemical plant. This approach has the advantage that consent does not have to be obtained, but it also has several disadvantages. First, it does not tell us how to determine adequate compensation. Second, it limits the freedom of individuals because some people would never have consented. Third, sometimes there is no adequate compensation for a harm, as in the case of serious injury or death.

There are problems with both informed consent and compensation as ways of dealing with the ethical requirement to respect the moral agency of those exposed to risk because of technology. Nevertheless, some effort must be made to honor this requirement. Now let us return to the second requirement of the respect-for-persons morality with regard to risk.

Equity and Justice

The ethics of respect for persons places great emphasis on respecting the moral agency of individuals, regardless of the cost to the larger society. Philosopher John Rawls expresses this concern:[27] "[E]ach member of society is thought to have an inviolability founded upon justice … which even the welfare of everyone else cannot override." As an example of the requirement for justice derived from the ethics of respect for persons, consider the following example from Cranor,[28] quoting a woman describing how her husband's health had been severely damaged by byssinosis caused by cotton dust:

> My husband worked in the cotton mill since 1937 to 1973. His breath was so short he couldn't walk from the parking lot to the gate the last two weeks he worked.
>
> He was a big man, liked fishing, hunting, swimming, playing ball, and loved to camp. We liked to go to the mountains and watch the bears. He got so he could not breathe and walk any distance, so we had to stop going anywhere. So we sold our camper, boat, and his truck as his doctor, hospital, and medicine bills were so high. We don't go anywhere now. The doctor said his lungs were as bad as they could get to still be alive. At first he used tank oxygen about two or three times a week, then it got so bad he used more and more. So now he has an oxygen concentrator, he has to stay on it 24 hours a day. When he goes to the doctor or hospital he has a little portable tank.
>
> He is bedridden now. It's a shame the mill company doesn't want to pay compensation for brown lung. If they would just come and see him as he is now, and only 61 years old.

A utilitarian might be willing to trade off the great harm to Mr. Talbert that resulted from a failure to force cotton mills to protect their workers from the risk of byssinosis for the smaller advantages to an enormous number of people. After all, such protection is often highly expensive and these expenses must eventually be passed on to consumers in the form of higher prices for cotton products. Higher prices also make U.S. cotton products more expensive and thus less competitive in world markets, thereby depriving U.S. workers of jobs. Regulations that protect workers might even force many (perhaps all) U.S. cotton mills to close. Such disutilities might well outweigh the disutilities to the Mr. Talberts of the world.

From the standpoint of the ethics of respect for persons, however, such considerations must not be allowed to obscure the fact that Mr. Talbert has been treated

unjustly. Although many people enjoy the benefits of the plant, only Mr. Talbert and a few others suffer the consequences of the unhealthy working conditions. The benefits and harms have been inequitably distributed. His rights to bodily integrity and life were unjustly violated. From the standpoint of the Golden Rule, probably few, if any, observers would want to be in Mr. Talbert's position.

Of course, it is not possible to distribute all risks and benefits equally. Sometimes those who endure the risks imposed by technology may not share the benefits to the same degree. For example, several years ago a proposal was made to build a port for unloading liquefied natural gas in the Gulf of Mexico off the coast of Texas. The natural gas would be shipped to many parts of the United States, so most citizens of the country would benefit from this project. Only those residents close to the port, however, would share the risks of the ships or storage tanks exploding.[29] Because there is no way to equalize the risk, informed consent and compensation should be important considerations in planning the project. Thus, informed consent, compensation, and equity are closely related considerations in moral evaluation.

Even though laypeople often combine the concept of risk with the concept of acceptable risk, we shall formulate a lay criterion of acceptable risk in the following way:

> An acceptable risk is one in which (1) risk is assumed by free and informed consent, or properly compensated, and in which (2) risk is justly distributed, or properly compensated.

We have seen that there are often great difficulties in implementing the requirements of free and informed consent, compensation, and justice. Nevertheless, they are crucial considerations from the layperson's perspective—and from the moral perspective.

6.5 COMMUNICATING RISK AND PUBLIC POLICY

Communicating Risk to the Public

The preceding sections show that different groups have somewhat different agendas regarding risk. Engineers are most likely to adopt the risk expert's approach to risk. They define risk as the product of the magnitude and likelihood of harm and are sympathetic with the utilitarian way of assessing acceptable risk. The professional codes require engineers to hold paramount the safety, health, and welfare of the public, so engineers have an obligation to minimize risk. However, in determining an acceptable level of risk for engineering works, they are likely to use, or at least be sympathetic with, the cost-benefit approach.

The lay public comes to issues of risk from a very different approach. Although citizens sometimes have inaccurate views about the probabilities of harms from certain types of technological risks, their different approach cannot be discounted in terms of simple factual inaccuracies. Part of the difference in approach results from the tendency to combine judgments of the likelihood and acceptability of risk. (The term "risky" seems to include both concepts.) For example, use of a technology is more risky if the technology is relatively new and if information about it comes from a source (either expert or nonexpert) that the public has come to regard as unreliable. More important, the lay public considers free and informed consent and equitable distribution of risk (or appropriate compensation) to be important in the determination of acceptable risk.

BOX 6.5 Communicating with the Public About Risks

- Use familiar terminology—"probability of harm" may be more clearly understood than "risk."
- Qualitatively compare "new" risks by comparison to "familiar" risks. "The probability of flooding related to the new development should not be greater than the present probability of flooding."
- Acknowledge uncertainty in risk assessments.
- Recognize that costs versus benefits are not the only factor in determining acceptability of risks.
- Be "objective and truthful" in all public statements.

In addition, government regulators, with their special obligation to protect the public from undue technological risks, are more concerned with preventing harm to the public than with avoiding claims for harm that turn out to be false. This bias contrasts to some extent with the agendas of both the engineer and the layperson. Although, as government regulators, they may often use cost-benefit analysis as a part of their method of determining acceptable risk, they have a special obligation to prevent harm to the public, and this may go beyond what cost-benefit considerations require. See Box 6.5 for different approaches when communicating with the public. On the other hand, considerations of free and informed consent and equity, while important, may be balanced by cost-benefit considerations.

In light of these three different agendas, it is clear that social policy regarding risk must take into consideration wider perspectives than the risk expert approach would indicate.

At least two reasons exist for this claim. First, the public and government regulators will probably continue to insist on introducing their own agendas into the public debate about technological risk. In a democracy, this probably means that these considerations will be a part of public policy regarding technological risk, whether or not engineers and risk experts approve. This is simply a fact to which engineers and risk experts must adjust. Second, we believe the two alternative approaches to risk each have a genuine moral foundation. Free and informed consent, equity, protecting the public from harm—these are morally legitimate considerations. Therefore, public policy regarding risk should probably be a mix of the considerations we have put forth here as well as, no doubt, many others we have not discussed.

What, then, is the professional obligation of engineers regarding risk? One answer is that engineers should continue to follow the risk expert's approach to risk and let public debate take care of the wider considerations. We believe there is some validity to this claim and in the next section we return to a consideration of issues in typical engineering approaches to risk. However, as we have argued in Chapter 3 and elsewhere, we believe engineers have a wider professional obligation. Engineers have a professional obligation to participate in democratic deliberation regarding risk by contributing their expertise to this debate. In doing so, they must be aware of alternative approaches and agendas to avoid serious confusion and undue dogmatism. In light of this, we propose the following guidelines for engineers in risk communication[30]:

1. Engineers, in communicating risk to the public, should be aware that the public's approach to risk is not the same as that of the risk expert. In particular, "risky" cannot be identified with a measure of the probability of harm. Thus,

engineers should not say "risk" when they mean "probability of harm." They should use the two terms independently.

2. Engineers should be wary of saying, "There is no such thing as zero risk." The public often uses "zero risk" to indicate not that something involves no probability of harm but that it is a familiar risk that requires no further deliberation.
3. Engineers should be aware that the public does not always trust experts and believes that experts have sometimes been wrong in the past. Therefore, engineers, in presenting risks to the public, should be careful to acknowledge the possible limitations in their position. They should also be aware that laypeople may rely on their own values in deciding whether or not to base action on an expert's prediction of probable outcomes.
4. Engineers should be aware that government regulators have a special obligation to protect the public and that this obligation may require them to take into account considerations other than a strict cost-benefit approach. Although public policy should take into account cost-benefit considerations, it should take into account the special obligations of government regulators.
5. Professional engineering organizations, such as the professional societies, have a special obligation to present information regarding technological risk. They must present information that is as objective as possible regarding probabilities of harm. They should also acknowledge that the public, in thinking about public policy regarding technological risk in controversial areas (e.g., nuclear power), may take into consideration factors other than the probabilities of harm.

A major theme in these guidelines is that engineers should adopt a critical attitude toward the assessment of risk. This means that they should be aware of the existence of perspectives other than their own. The critical attitude also implies that they should be aware of the limitations in their own abilities to assess the probabilities and magnitude of harms. In the next section, we consider an example of these limitations and the consequent need for the critical attitude even in looking at the mode of risk assessment characteristic of engineering.

An Example of Public Policy: Building Codes

One of the most immediate ways in which public policy must rely on engineering expertise and engineering is in turn affected by public policy is through local building codes. The local building codes specify design rules that incorporate factors of safety and construction steps (e.g., fireproofing or material requirements) that are required in the area. Building codes have the status of law and may not be changed without public hearings and legislative action. The legislature will often appoint a committee of experts to propose a new building code or necessary changes in an existing one. For example, following the collapse of the World Trade Center's Twin Towers, there was a major multiagency investigative effort to identify the causes of the collapses and to propose changes in New York City's building codes that would improve egress and otherwise reduce risks of death.

One of the more important ways professional engineers show a concern for the general public (and their safety) is in carrying out the local building code requirements in designing such things as buildings, elevators, escalators, bridges, walkways, roads, and overpasses. When a responsible engineer recognizes a violation of a

building code in a design and does not object to it, the engineer bears some responsibility for any injuries or deaths that result. Similarly, when an engineer learns of a proposed change in a building code that he or she is convinced creates danger for the public and does nothing to prevent this change, the engineer bears some responsibility for any harm done.

The Twin Towers case illustrates these issues.[31] The New York City building codes in place in 1945 required that all stairwells be surrounded with heavy masonry and concrete structure. Consequently, in 1945, firefighters were able to get to the area inside the Empire State Building immediately through the stairwells and put out the fire in 40 minutes. In the intervening years between the design of the Empire State Building and the World Trade Center Towers, building codes underwent a general change nationwide, with the "prescriptive" code requirements tending to be replaced by "performance" code requirements. One example is the way fireproofing coatings for steel structural members were specified in the early codes. Then, a certain thickness of concrete was specified, but as improved materials for fireproofing evolved that resulted in lower dead loads and more economical application methods, codes were changed to specify instead a certain level of performance. Similar changes in high-rise construction materials and methods, such as the use of lightweight concrete floor slabs and lighter floor joist systems, helped make taller structures more affordable. Some of these more economical and lighter weight building components may have been factors in the very different performance of the two newer towers compared to the much heavier Empire State Building and some critics have suggested we should revert to the older technology for tomorrow's buildings.

But reverting to 50-year-old practices is not the answer, nor is it even feasible. Rather it is up to today's engineers to help maintain performance standards in model building codes that will produce structures that are affordable without introducing unacceptable risk to the public they will serve. The Federal Emergency Management Agency (FEMA) and the Structural Engineering Institute of the American Society of Civil Engineers studied building code issues related to the WTC collapses and loss of life and concluded that the structures performed well in response to the crash impact loadings and continued standing even after the resulting severe damage, which is a testament to their design, but the resulting fire started by the approximately 10,000 gallons of burning jet fuel was further fed by building furnishings and materials of construction causing temperatures too high for the structural steel members given the mechanical damage to the fire protection systems. While the fire protection features of the design and construction were found to meet or exceed minimum code requirements, the study recommends more detailed evaluation of several features for future building code requirements, including floor truss systems and their robustness, impact resistant enclosures around egress paths, resistance of fire protection to physical damage, and location of egress paths. But the authors of the study did not recommend specific requirements to harden structures against aircraft impact, concluding that "it may not be technically feasible to develop design provisions that would enable all structures to be designed and constructed to resist the effects of impacts by rapidly moving aircraft, and the ensuing fires, without collapse."

As another example of a serious shortcoming of the New York City building codes, see the Citicorp building case in the Appendix. In this case, William LeMessurier designed the building's main load-carrying steel structure to a code-specified worst-case wind condition that was incorrect. Fortunately, LeMessurier recognized

the error in the code and modified the already built structure to correct for it. The codes were subsequently corrected.

Building codes are one of the aspects of public policy that both directly affect engineers and most clearly require information from engineers in their formulation. They illustrate one of the most concrete and specific ways in which engineering expertise is needed in the formulation of public policy and in which public policy in turn vitally affects engineering design.

6.6 THE ENGINEER'S LIABILITY FOR RISK

We have seen that risk is difficult to estimate and that engineers are often tempted to allow anomalies to accumulate without taking remedial action and even to expand the scope of acceptable risk to accommodate them. We have also seen that there are different and sometimes incompatible approaches to the definition of acceptable risk as exhibited by risk experts, laypeople, and government regulators.

Another issue that raises ethical and professional concerns for engineers regards legal liability for risk. There are at least two issues here. One is that the standards of proof in tort law and science are different and this produces an interesting ethical conflict. Another issue is that in protecting the public from unnecessary risk, engineers may themselves incur legal liabilities. Let us consider each of these issues.

The Standards of Tort Law

Litigation that seeks redress from harm most commonly appeals to the law of torts, which deals with injuries to one person caused by another, usually as a result of fault or negligence of the injuring party. Many of the most famous legal cases involving claims of harm from technology have been brought under the law of torts. The litigation involving harm from asbestos is one example. In 1973, the estate of Clarence Borel,[32] who began working as an industrial insulation worker in 1936, brought suit against Fiberboard Paper Products Corporation:

> During his career he was employed at numerous places usually in Texas, until disabled from the disease of asbestosis in 1969. Borel's employment necessarily exposed him to heavy concentrations of asbestos generated by insulation materials. In a pretrial deposition Borel testified that at the end of the day working with insulation materials containing asbestos his clothes were usually so dusty that he could barely pick them up without shaking them. Borel stated, "You just move them a little bit and there is going to be dust and I blowed this dust out of my nostrils by the handfuls at the end of the day. I even used Mentholatum in my nostrils to keep some of the dust from going down my throat, but it is impossible to get rid of all of it. Even your clothes just stay dusty continuously, unless you blow it off with an air hose." In 1964, doctors examined Borel in connection with an insurance policy and informed him that x-rays of his lungs were cloudy. The doctors told Borel that the cause could be his occupation as an installation worker and advised him to avoid asbestos dust as much as he possibly could. On January 19, 1969, Borel was hospitalized and a lung biopsy was performed. Borel's condition was diagnosed as pulmonary asbestosis. Since the disease was considered irreversible Borel was sent home.... [His] condition gradually worsened during the remainder of 1969. On February 11, 1970, he underwent surgery for the removal of his right lung. The examining doctors determined that Borel had a form of lung cancer known as mesothelioma, which had been caused by asbestos. As a result of these diseases, Borel later died before the district case reached the trial stage.[33]

The federal district court in Texas decided in favor of the estate of Mr. Borel and the Fifth Circuit Court of Appeals upheld the decision.

The standard of proof in tort law is the preponderance of evidence, meaning that there is more and better evidence in favor of the plaintiff than the defendant. The plaintiff must show

> (1) that the defendant violated a legal duty imposed by the tort law, (2) that the plaintiff suffered injuries compensable in the tort law, (3) that the defendant's violation of legal duty caused the plaintiff's injuries, and (4) that the defendant's violation of legal duty was the proximate cause of the plaintiff's injuries.[34]

The standard of proof that a given substance was the proximate cause of a harm is less stringent than that which would be demanded by a scientist, who might well call for 95 percent certainty. It is also less stringent than the standard of evidence in criminal proceedings, which calls for proof beyond reasonable doubt.

As an illustration of this lower standard of evidence, consider the case of *Rubanick v. Witco Chemical Corporation and Monsanto Co.* The plaintiff's sole expert witness, a retired cancer researcher at New York's Sloan-Kettering Cancer Center, testified that the deceased person's cancer was caused by exposure to polychlorinated biphenyls (PCBs). He based his opinion on

> (1) the low incidence of cancer in males under 30 (the deceased person was 29), (2) the decedent's good dietary and nonsmoking habits and the absence of familial genetic predisposition to cancer, (3) 5 of 105 other Witco workers who developed some kind of cancer during the same period, (4) a large body of evidence showing that PCBs cause cancer in laboratory animals, and (5) support in the scientific literature that PCBs cause cancer in human beings.[35]

The court did not require the expert to support his opinion by epidemiological studies, merely that he demonstrate the appropriate education, knowledge, training, and experience in the specific field of science and an appropriate factual basis for his opinion.[36]

Courts in other better known cases, such as that of Richard Ferebee, who alleged that he suffered lung damage as a result of spraying the herbicide paraquat, also accepted standards of evidence for causal claims that would not have been acceptable for research purposes.[37]

Some courts, however, have begun to impose higher standards of evidence for recovery of damages through tort standards that are similar to those used in science. In the Agent Orange cases, Judge Jack B. Weinstein argued that epidemiological studies were the only useful studies having any bearing on causation, and that by this standard no plaintiff had been able to make a case. Bert Black,[38] a legal commentator, has taken a similar view. He believes that the courts (i.e., judges) should actively scrutinize the arguments of expert witnesses, demanding that they be supported by peer-reviewed scientific studies or at least have solid scientific backing. In some cases, he believes, they should even overrule juries who have made judgments not based on scientific standards of evidence.[39]

Even though this view represents a departure from the normal rules of evidence in tort law, it might in some cases be fairer to the defendants because some decisions in favor of plaintiffs may not be based on valid proof of responsibility for harm. The disadvantage is also equally obvious. By requiring higher standards of proof, the

courts place burdens of evidence on plaintiffs that they often cannot meet. In many cases, scientific knowledge is simply not adequate to determine causal relationships, and this would work to the disadvantage of the plaintiffs. There are also problems with encouraging judges to take such an activist role in legal proceedings. The major ethical question, however, is whether we should be more concerned with protecting the rights of plaintiffs who may have been unjustly harmed or with promoting economic efficiency and protecting defendants against unjust charges of harm. This is the ethical issue at the heart of the debate.

The above discussion assumes it is the engineer's decision about what risk is acceptable that is challenged in court. It is also possible, and perhaps more common, that the claim does not dispute the engineer's decision about what risk is acceptable, but rather claims that the engineer has made a design error, or neglected to consider some factor affecting the risk, which has led to a greater than acceptable risk and to some injury.

Some Problems with Tort Law

The apparent ease with which proximate cause can be established in tort law may suggest that the courts should impose a more stringent standard of acceptable risk. But other aspects of the law afford the public less protection than it deserves. For example, the threat of legal liability can inhibit engineers from adequately protecting the public from risk. Engineers in private practice may face especially difficult considerations regarding liability and risk, and in some cases they may need increased protection from liability.

Consider, for example, the safety issues in excavating for foundations, pipelines, and sewers.[40] A deep, steep-sided trench is inherently unstable. Sooner or later, the sidewalls will collapse. The length of time that trench walls will stand before collapsing depends on several factors, including the length and width of the cut, weather conditions, moisture in the soil, composition of the soil, the method of excavation, and the nearby presence of heavy or vibrating equipment. People who work in deep trenches are subjected to considerable risk, and hundreds of laborers are injured or killed each year when the walls collapse.

To reduce the risk, construction engineers can specify the use of trench boxes in their designs. A trench box is a long box with an upside-down U-shaped cross section that is inserted inside the trench to protect the laborers. As long as workers remain inside the trench boxes, their risk of death or injury is greatly reduced.

Unfortunately, the use of trench boxes considerably increases the expense and time involved in construction projects. The boxes must be purchased or rented, and then they must be moved as excavation proceeds, slowing construction work and adding further expense. In addition, the handling of trench boxes introduces another risk of injury to workers involved. Engineers are placed in an awkward position with regard to the use of trench boxes, especially where the boxes are not required by building codes. If they do not specify the use of the boxes, then they may be contributing to a situation that subjects workers to a high risk of death and injury. If they do specify the use of boxes, then they may be incurring liability in case of an accident because of the use of trench boxes. With situations such as this in mind, the National Society of Professional Engineers has been actively lobbying the U.S. Congress to pass a law that specifically excludes engineers from liability for accidents where construction safety measures are specified by engineers but then are either not

used or used improperly by others. This would enable engineers more effectively to protect the safety of workers. Unfortunately, the proposals have never become law.

The problem with trench boxes illustrates a more general issue. If engineers were free to specify safety measures without being held liable for their neglect or improper use, they could more easily fulfill one aspect of their responsibility to protect the safety of the public.

Protecting Engineers from Liability

Engineers face two problems in terms of their liability for injuries or damages under tort law. First, they may have to defend their assessment and management of a risk that they deemed to be acceptable, which has later resulted in an injury. Second, they may have to defend their work against a claim that they erred in some calculation or neglected to consider some aspect of a risk. An effective defense against either type of claim requires good records of engineering design and management decisions. A daily journal that records the essence of each meeting or conversation can be invaluable in demonstrating that errors were not made and important issues were not overlooked. And, the purchase of an "errors and omissions" insurance policy is important as protection for those instances in which such an error or omission does lead to a harm. After all, a responsible engineer would not want to be unable to compensate for damage or an injury resulting from an error or oversight.

It is also important that engineers understand and adhere to the "standard of care" expected in tort law to counter claims of negligence or incompetence. The standard of care is a legal standard for engineering decision-making defined by the ordinary skill, competence, and diligence exercised by qualified engineers practicing in a given field. Under the standard of care, engineers are not expected to be perfect or error-free, rather to be as competent and careful as other practitioners involved in the same work. Negligence, specifically failing to exercise the same diligence as other practitioners, is an important factor in establishing liability. It is also important to understand the standard of care when promoting engineering services. An engineer who describes his or her services using adjectives such as "leading edge" or touting "highest professional standards" of practice might invite an argument that a client was justified in expecting a higher standard of care.

6.7 BECOMING A RESPONSIBLE ENGINEER REGARDING RISK

The first step in the process of becoming ethically responsible about risk is to be aware of the fact that risk is often difficult to estimate and can be increased in ways that may be subtle and treacherous. The second step is to be aware that there are different approaches to the determination of acceptable risk. In particular, engineers have a strong bias toward quantification in their approach to risk, which may make them insufficiently sensitive to the concerns of the lay public and even the government regulators. The third step is to assume their responsibility, as the experts in technology, to communicate issues regarding risk to the public, with the full awareness that both the public and government regulators have a somewhat different agenda with regard to risk.

We conclude with an attempt to formulate a principle of acceptable risk. To formulate this principle, let us consider further some of the legal debate about risk.

The law seems to be of two minds about risk and benefits. On the one hand, some laws make no attempt to balance the two. The Chemical Food Additives Amendments to the Food, Drug and Cosmetics Act, enacted in 1958, require that a chemical "deemed to be unsafe" not be added to food unless it can be "safely used."[41] Safe use was defined by the Senate Committee on Labor and Public Welfare as meaning that "no harm will result" from its addition to food.[42] The well-known Delaney Amendment also prohibits the addition to food of any chemical known to cause cancer when ingested by animals.[43]

On the other hand, there is often an attempt to strike a balance between the welfare of the public and the rights of individuals. The Toxic Substances Control Act of 1976 authorized the EPA to regulate any chemical upon a finding of "unreasonable risk of injury to health or the environment."[44] But it is only "unreasonable risk" that triggers regulation, so some degree of risk is clearly tolerated. The report of the House Commerce Committee describes this balancing process as follows:

> Balancing the probabilities that harm will occur and the magnitude and severity of that harm against the effect of proposed regulatory action on the availability to society of the benefits of the substance or mixture, taking into account the availability of substitutes for the substance or mixture which do not require regulation, and other adverse effect which such proposed action may have on society.

Having said this, the report goes on to say that "a formal benefit-cost analysis under which monetary value is assigned to the risks … and to the costs of society" is not required.[45]

The Atomic Energy Act of 1954 continually refers to the "health and safety of the public" but makes little attempt to define these terms. The Nuclear Regulatory Commission's rules, however, use the expression "without undue risk" and seem to suggest again a balancing of risks and benefits.[46] In the words of one legal commentator, in practice, especially in the earlier years, "the acceptability of risk was measured largely in terms of the extent to which industry was capable of reducing the risk without jeopardizing an economic and financial environment conducive to continuing development of the technology."[47] Again, we have an attempt to balance protection of individuals and promotion of the public welfare.

Sometimes the conflict between these two approaches is evident in a single debate. In a Supreme Court case involving exposure to benzene in the workplace, OSHA took an essentially respect for persons standpoint, arguing that the burden of proof should be on industry to prove that a given level of exposure to benzene was not carcinogenic. In its rebuke of OSHA, the Supreme Court argued that in light of the evidence that current standards did not lead to harm to workers, risk must be balanced against benefits in evaluating more stringent standards and that the burden of proof was on OSHA to show that the more stringent standards were justified.[48]

Given these considerations, we can construct a more general principle of acceptable risk, which may provide some guidance in determining when a risk is within the bounds of moral permissibility:

> People should be protected from the harmful effects of technology, especially when the harms are not consented to or when they are unjustly distributed, except that this protection must sometimes be balanced against (1) the need to preserve great and irreplaceable benefits, and (2) the limitation on our ability to obtain informed consent.

The principle does not offer an algorithm that can be applied mechanically to situations involving risk. Many issues arise in its use; each use must be considered on its own merits. We can enumerate some of the issues that arise in applying the principle.

First, we must define what we mean by "protecting" people from harm. This cannot mean that people are assured that a form of technology is free from risk. At best, "protection" can only be formulated in terms of probabilities of harm and we have seen that even these are subject to considerable error.

Second, many disputes can arise as to what constitutes a harm. Is having to breathe a foul odor all day long harm? What about workers in a brewery or a sewage disposal plant? Here the foul odors cannot be eliminated, so the question of what harms should be eliminated cannot be divorced from the question of whether the harms can be eliminated without at the same time eliminating other goods.

Third, the determination of what constitutes a great and irreplaceable benefit must be made in the context of particular situations. A food additive that makes the color of frozen vegetables more intense is not a great and irreplaceable benefit. If such an additive were found to be a powerful carcinogen, then it should be eliminated. On the other hand, most people value automobiles highly and they would probably not want them to be eliminated, despite the possibility of death or injury from automobile accidents.

Fourth, we have already pointed out the problems that arise in determining informed consent and the limitations in obtaining informed consent in many situations. From the standpoint of the ethics of respect for persons, informed consent is a consideration of great importance. However, it is often difficult to interpret and apply.

Fifth, the criterion of unjust distribution of harm is also difficult to apply. Some harms associated with risk are probably unjustly distributed. For example, the risks associated with proximity to a toxic waste disposal area that is not well constructed or monitored are unjustly distributed. The risks associated with coal mining might also be conceded to be unjustly distributed, but the energy provided by coal may also be considered a great and irreplaceable benefit. So the requirement to reduce risk in the coal industry might be that the risks of coal mining should be reduced as much as possible without destroying the coal industry. This might require raising the price of coal enough to make coal mining safe and more economically rewarding.

Sixth, an acceptable risk at a given point in time may not be an acceptable risk at another point in time. Engineers with operational responsibilities as well as those with design responsibilities have an obligation to protect the health and safety of the public. This obligation requires engineers to reduce risk when new risks emerge or when risk awareness or acceptability changes or even when technological innovation allows further reduction of known risks. This obligation was not recognized or discharged by operators or regulators at the Fukushima nuclear power plant, where the improved predictions of tsunami risks should have triggered countermeasures.

6.8 CHAPTER SUMMARY

Risk is a part of engineering and especially of technological progress. The concept of "factors of safety" is important in engineering. Virtually all engineering codes give a prominent place to safety. Engineers and risk experts look at risk in a somewhat

different way from others in society. For engineers, risk is the product of the probability and magnitudes of harm. Acceptable levels of risk represent public policy and are generally determined by groups of experts based on historical practices. Acceptable risks are implemented in building codes or design standards or in standardized operational practices. When other guidance is not available, an acceptable risk might be defined as one in which the product of the probability and magnitude of the harm is equaled or exceeded by the product of the probability and magnitude of the benefit and no other option exists where the product of the probability and magnitude of the benefit is substantially greater, although this approach might result in unacceptable inequities in risk distributions. In calculating harms and benefits, engineers have traditionally identified harm with factors that are relatively easily quantified, such as economic losses and loss of life. The "capabilities" approach attempts to make these calculations more sophisticated by developing a more adequate way of measuring the harms and benefits from disasters to overall well-being, which it defines in terms of the capabilities of people to live the kind of life they value. A risk is acceptable if the probability is sufficiently small that the adverse effect of a hazard will fall below a threshold of the minimum level of capabilities attainment that is acceptable in principle.

The public does not conceptualize risk simply in terms of expected deaths or injury but, rather, considers other factors as well, such as whether the harm in question is unacceptably severe, whether a risk is assumed with free and informed consent or whether the risk is imposed justly. Government regulators still take a different approach to risk because they have a special obligation to protect the public from harm. Consequently, they place greater weight on protecting the public than on benefiting the public. In light of these different agendas, social policy must take into account a wider perspective than that of the risk expert.

Engineers, and especially professional engineering societies, have an obligation to contribute to public debate on risk by supplying expert information and by recognizing that the perspectives in the public debate will comprise more than the perspective of the risk expert. Debates over building codes illustrate some aspects of this public debate over risk.

Estimating the causes and likelihood of harm poses many difficulties. Engineers use various techniques, such as fault trees and event trees. However, the phenomena of "tight coupling" and "complex interactions" limit our ability to anticipate disasters. The tendency to accept increasing deviations from expected performance can also lead to disasters.

Engineers need to protect themselves from undue liability for risk, but this need sometimes raises important issues for social policy. One issue is the conflict between the standards of science and tort law. The standard of proof in tort law for whether something causes a harm is the preponderance of evidence, but the standard of evidence in science is much higher. The lower standard of tort law tends to protect the rights of plaintiffs who may have been unjustly harmed, and the higher standard of science tends to protect defendants and perhaps promote economic efficiency. The problems engineers have in protecting themselves from unjust liabilities while protecting the public from harm are illustrated by the use of trench boxes. Finally, a principle of acceptable risk provides some guidance in determining when a risk is within the bounds of moral permissibility.

NOTES

1. "B-25 Crashes in Fog," *New York Times*, July 29, 1945, p. 1.
2. Peter Glantz and Eric Lipton, "The Height of Ambition," *New York Times Sunday Magazine*, September 8, 2002, p. 32.
3. Z. Bazant and M. Verdure, "Mechanics of Progressive Collapse: Learning from World Trade Center and Building Demolitions," *Journal of Engineering Mechanics*, ASCE, March 2007, pp. 308–319.
4. J. M. Acton, *Why Fukushima Was Preventable* (Washington, DC: Carnegie Endowment for International Peace, 2012). Retrieved November 2016, from http://carnegieendowment.org/files/fukushima.pdf
5. ASCE Hurricane Katrina External Review Panel, *The New Orleans Hurricane Protection System: What Went Wrong and Why* (Reston, Virginia: American Society of Civil Engineers, 2007). Retrieved February 27, 2017, from http://biotech.law.lsu.edu/katrina/reports/EPRreport.pdf
6. For further discussion of the concept of capabilities and description of this approach to measuring harm in this section, see Amartya Sen, *Development as Freedom* (New York: Anchor Books, 1999); Martha Nussbaum, *Women and Human Development: The Capabilities Approach* (New York: Cambridge University Press, 2000); Colleen Murphy and Paolo Gardoni, "The Role of Society in Engineering Risk Analysis: A Capabilities-Based Approach," *Risk Analysis*, 26, no. 4, pp. 1073–1083; and Colleen Murphy and Paolo Gardoni, "The Acceptability and the Tolerability of Societal Risks: A Capabilities-based Approach," *Science and Engineering Ethics*, 14, no. 1, 2008, pp. 77–92. We are indebted to Professors Murphy and Gardoni for supplying the basis of this section.
7. S. Anand and Amartya Sen, "The Income Component of the Human Development Index," *Journal of Human Development*, 1, no. 1, 2000, 83–106.
8. Colleen Murphy and Paolo Gardoni, "Determining Public Policy and Resource Allocation Priorities for Mitigating Natural Hazards; A Capabilities-based Approach," *Science & Engineering Ethics*, 13, no. 4, 2007, pp. 489–504.
9. Colleen Murphy and Paolo Gardoni, "The Acceptability and the Tolerability of Societal Risks: A Capabilities-Based Approach," *Science and Engineering Ethics*, 14, no. 1, 2008, pp. 77–92.
10. Cranor, *Regulating Toxic Substances*, p. 11.
11. World Nuclear Association Web page on Fukushima Accident 2011, updated April 14, 2012, found at http://www.world-nuclear.org/info/fukushima_accident_inf129.html
12. Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, 1984), p. 3.
13. See New York Times, October 15, 1962, for an account of this tragic event. The engineering details are cited from an unpublished report by R. C. King, H. Margolin, and M. J. Rabins to the City of New York Building Commission on the causes of the accident.
14. Diane Vaughn, *The Challenger Launch Decision* (Chicago: University of Chicago Press, 1996), pp. 409–422.
15. See the Presidential Commission on the Space Shuttle *Challenger* Accident, "Report to the President by the Presidential Commission on the Space Shuttle *Challenger* Accident."
16. See Vaughn, *The Challenger Launch Decision*, pp. 110–111. The following account is taken from Vaughn and from personal conversations with Roger Boisjoly. This account should be attributed to the authors, however, rather than to Diane Vaughn or Roger Boisjoly.
17. Ibid., pp. 121 ff.
18. Ibid., pp. 141 ff.
19. Ibid., pp. 153 ff.

20. The National Public Radio story was aired on "Morning Edition," December 3, 1992. This account is taken from the Newsletter of the Center for Biotechnology Policy and Ethics, Texas A & M University, 2:1, January 1, 1993, p. 1.
21. Chauncey Starr, "Social Benefits versus Technological Risk," Science, 165, September 19, 1969, pp. 1232–1238. Reprinted in Theodore S. Glickman and Michael Gough, *Readings in Risk* (Washington, DC: Resources for the Future), pp. 183–193.
22. Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein, "Rating the Risks," Environment, 21, no. 3, April 1969, pp. 14–20, 36–39. Reprinted in Glickman and Gough, pp. 61–74.
23. Starr, "Social Benefits versus Technological Risk," pp. 183–193.
24. For this and several of the following points, see Paul B. Thompson, "The Ethics of Truth-Telling and the Problem of Risk," *Science and Engineering Ethics*, 5, 1999, pp. 489–510.
25. Starr, op. cit., pp. 183–193.
26. D. Litai, "A Risk Comparison Methodology for the Assessment of Acceptable Risk," PhD dissertation, Massachusetts Institute of Technology, Cambridge, MA, 1980.
27. John Rawls, *A Theory of Justice* (Cambridge, MA: Harvard University Press, 1971), p. 3.
28. Carl F. Cranor, *Regulating Toxic Substances: A Philosophy of Science and the Law* (New York: Oxford University Press, 1993), p. 152.
29. Ralph L. Kenny, Ram B. Kulkarni, and Keshavan Nair, "Assessing the Risks of an LGN Terminal," in Glickman and Gough, pp. 207–217.
30. This list was suggested by the four "dicta for risk communication" proposed by Paul Thompson, in Thompson, op. cit., pp. 507–508. Although some items in this list are the same as Thompson's, we have modified and expanded his list.
31. World Trade Center Building Performance Study: Data Collections, Preliminary Observations and Recommendations, FEMA 403, Federal Emergency Management Agency, Federal Insurance and Mitigation Administration, Washington, DC, September 2002.
32. *Borel v. Fiberboard Paper Products Corp.* et al., 493 F.2d (1973) at 1076, 1083. Quoted in Cranor, Regulating Toxic Substances, p. 52.
33. Cranor, *Regulating Toxic Substances*, p. 58.
34. 576 A.2d4 (N.J. Sup. Ct. A.D.1990) at 15 (concurring opinion).
35. Cranor, *Regulating Toxic Substances*, p. 81. Summarized from "New Jersey Supreme Court Applies Broader Test for Admitting Expert Testimony in Toxic Case," *Environmental Health Letter*, August 27, 1991, p. 176.
36. "New Jersey Supreme Court Applies Broader Test," p. 176.
37. *Ferebee v. Chevron Chemical Co.*, 736 F.2d 11529 (D.C. Cir 1984).
38. Bert Black, "Evolving Legal Standards for the Admissibility of Scientific Evidence," *Science*, 239, 1987, pp. 1510–1512.
39. Bert Black, "A Unified Theory of Scientific Evidence," *Fordham Law Review*, 55, 1987, pp. 595–692.
40. See R. W. Flumerfelt, C. E. Harris, Jr., M. J. Rabins, and C. H. Samson, Jr., Introducing Ethics Case Studies into Required Undergraduate Engineering Courses, Final Report to the NSF on Grant DIR-9012252, November 1992, pp. 262–285.
41. Public Law No. 85-929, 72 Stat. 784 (1958).
42. Senate Report No. 85-2422, 85th Congress, 2nd Session (1958).
43. c21 United States Code, sect. 348 (A) (1976).
44. Public Law No. 94-469, 90 Stat. 2003 (1976). The same criterion of "unreasonable risk" is found in the Flammable Fabrics Act. See Public Law No. 90-189, Stat. 568 (1967).
45. Public Law No. 83-703, 68 Stat. 919 (1954), 42 United States Code 2011 et. seq. (1976).
46. 10 CFR 50.35 (a) (4).
47. Harold P. Green, "The Role of Law in Determining Acceptability of Risk," in *Societal Risk Assessment: How Safe Is Safe Enough?* (New York: Plenum, 1980), p. 265.
48. *Industrial Union Department, AFL-CIO v. American Petroleum Institute* et al., 448 U.S. 607 (1980).