PART II

THE EXPERIMENTAL NATURE OF ENGINEERING

To undertake a great work, and especially a work of a novel type, means carrying out an experiment. It means taking up a struggle with the forces of nature without the assurance of emerging as the victor after the first attack.

Louis Marie Henri Navier (1785–1836)
a founder of structural analysis

A ship in harbor is safe, but that is not what ships are built for.

John A. Shedd

Primum non nocere. (Above all, do no harm.)

Admonition to Physicians

CHAPTER 3

ENGINEERING AS SOCIAL EXPERIMENTATION

As it departed on its maiden voyage in April 1912 the *Titanic* was proclaimed the greatest engineering achievement ever. Not merely was it the largest ship the world had seen, having a length of two and a half football fields, it was also the most glamorous of ocean liners, complete with a tropical vinegarden restaurant and the first seagoing masseuse. It was supposed to be the first fully safe ship. Since the worst collision envisaged was at the juncture of two of its sixteen watertight compartments, and since it could float with any four compartments flooded, the *Titanic* was confidently believed to be virtually unsinkable.

Buoyed by such confidence, the captain allowed the ship to sail full speed at night in an area of reported icebergs, one of which tore a large gap in its side, directly or indirectly* flooding five compartments. Time remained to evacuate the ship, but there were not enough lifeboats to accommodate all the passengers and crew. British regulations then in effect did not foresee vessels of this size. Accordingly only 825 places were required in lifeboats, sufficient for a mere one-quarter of the *Titanic*'s capacity of 3547 passengers and crew. No extra precautions had seemed necessary for a practically unsinkable ship. The result: 1522 dead (drowned or frozen) out of the 2227 on board for the *Titanic*'s first trip (Lord, 1976; Wade, 1980; Davie, 1986).

In his poem written shortly after the event, "The Convergence of the Twain," Thomas Hardy portrayed the meeting of the ship and iceberg as de-

*Some investigators believe the *Titanic* left England with a coal fire on board, that this made the captain rush the ship to New York, and that water entering the coal bunkers through the gash caused an explosion and thereby greater damage to the compartments.

termined by unpredictable fate: "No mortal eye could see/The intimate welding of their later history." Yet greater imagination and prudence could have prevented the disaster.

Interestingly enough, novelists did not lack the imaginative foresight to describe scenarios that paralleled the later real events in shocking detail. In Morgan Robertson's 1898 novel *Futility*, a ship almost identical in size to the *Titanic* was wrecked by an iceberg on a cold April night. The ship in the book was named the *Titan;* it too had a less than sufficient number of lifeboats. Mayn Clew Garnett's story "The White Ghost of Disaster" was being readied for publication in *Popular Magazine* while the *Titanic* was on her maiden voyage. It is said that Garnett had dreamed the story while traveling on the *Titanic*'s sister ship, the *Olympic*. Again, circumstances similar to those surrounding the sinking of the *Titanic*, as well as an insufficient number of lifeboats to save all the passengers, were key elements in the narrative (Wade, 1980, 70–71).

The *Titanic* remains a haunting image of technological complacency. Perhaps all we can take for granted today is Murphy's law that if anything can go wrong, it will—sooner or later. All products of technology present some potential dangers, and thus engineering is an inherently risky activity. In order to underscore this fact and help in exploring its ethical implications, we suggest that engineering should be viewed as an experimental process. It is not, of course, an experiment conducted solely in a laboratory under controlled conditions. Rather, it is an experiment on a social scale involving human subjects.

ENGINEERING AS EXPERIMENTATION

Experimentation is commonly recognized to play an essential role in the design process. Preliminary tests or simulations are conducted from the time it is decided to convert a new engineering concept into its first rough design. Materials and processes are tried out, usually employing formal experimental techniques. Such tests serve as the basis for more detailed designs, which in turn are tested. At the production stage further tests are run, until a finished product evolves. The normal design process is thus iterative, carried out on trial designs with modifications being made on the basis of feedback information acquired from tests. Beyond those specific tests and experiments, however, each engineering project taken as a totality may itself be viewed as an experiment.

Similarities to Standard Experiments

Several features of virtually every kind of engineering practice combine to make it appropriate to view engineering projects as experiments. First, any project is carried out in partial ignorance. There are uncertainties in the ab-

stract model used for the design calculations; there are uncertainties in the precise characteristics of the materials purchased; there are uncertainties about the nature of the stresses the finished product will encounter. Engineers do not have the luxury of waiting until all the relevant facts are in before commencing work. At some point theoretical exploration and laboratory testing must be bypassed for the sake of moving ahead on a project. Indeed, one talent crucial to an engineer's success lies precisely in the ability to accomplish tasks with only a partial knowledge of scientific laws about nature and society.

Second, the final outcomes of engineering projects, like those of experiments, are generally uncertain. Often in engineering it is not even known what the possible outcomes may be, and great risks may attend even seemingly benign projects. A reservoir may do damage to a region's social fabric or to its ecosystem. It may not even serve its intended purpose if the dam leaks or breaks. An aqueduct may bring about a population explosion in a region where it is the only source of water, creating dependency and vulnerability without adequate safeguards. An aircraft may become a status symbol that ultimately bankrupts its owners. A special-purpose fingerprint reader may find its main application in the identification and surveillance of dissidents by totalitarian regimes. A nuclear reactor, the scaled-up version of a successful smaller model, may exhibit unexpected problems that endanger the surrounding population, leading to its untimely shutdown at great cost to owner and consumers alike. A hair dryer may expose the unknowing or unwary user to lung damage from the asbestos insulation in its barrel.

Third, effective engineering relies upon knowledge gained about products both before and after they leave the factory—knowledge needed for improving current products and creating better ones. That is, ongoing success in engineering depends upon gaining new knowledge, just as does ongoing success in experimentation. Monitoring is thus as essential to engineering as it is to experimentation in general. *To monitor* is to make periodic observations and tests in order to check for both successful performance and unintended side effects. But since the ultimate test of a product's efficiency, safety, cost-effectiveness, environmental impact, and aesthetic value lies in how well that product functions within society, monitoring cannot be restricted to the development or testing phases of an engineering venture. It also extends to the stage of client use. Just as in experimentation, both the intermediate and final results of an engineering project deserve analysis if the correct lessons are to be learned from it.

Learning from the Past

It might be expected that engineers would learn not only from their own earlier design and operating results, but also from those of other engineers. Unfortunately that is frequently not the case. Lack of established channels of communication, misplaced pride in not asking for information, embarrass-

ment at failure, and plain neglect often impede the flow of such information and lead to many repetitions of past mistakes. Here are a few examples:

1 The *Titanic* lacked a sufficient number of lifeboats decades after most of the passengers and crew on the steamship *Arctic* had perished because of the same problem (Wade, 1980, 417).

2 "Complete lack of protection against impact by shipping caused Sweden's worst ever bridge collapse on Friday as a result of which eight people were killed." Thus reported the *New Civil Engineer* on January 24, 1980. On May 15 of the same year it also reported the following: "Last Friday's disaster at Tampa Bay, Florida, was the largest and most tragic of a growing number of incidents of errant ships colliding with bridges over navigable waterways." While collisions of ships with bridges do occur—other well-known cases being those of the Maracaibo Bridge (Venezuela, 1964) and the Tasman Bridge (Australia, 1975)—Tampa's Sunshine Skyline Bridge was not designed with horizontal impact forces in mind because the code did not require it. Floating concrete bumpers which can deflect ships have been proposed by Laura and Nava (1981).

3 In June 1966 a section of the Milford Haven bridge in Wales collapsed during construction. A bridge of similar design was being erected by the same bridge builder (Freeman Fox and Partners) in Melbourne, Australia, when it too partially collapsed, killing thirty-three people and injuring nineteen. This happened in October of the same year, shortly after chief construction engineer Jack Hindshaw (also a casualty) had assured worried workers that the bridge was safe (Yarrow Bridge, 415).

4 Valves are notorious for being among the least reliable components of hydraulic systems. It was a pressure relief valve, and lack of positive information regarding its open or shut state, which helped lead to the nuclear reactor accident at Three Mile Island on March 28, 1979. Similar malfunctions had occurred with identical valves on nuclear reactors at other locations. The required reports had been filed with Babcock and Wilcox, the reactor's manufacturer, but no attention had been given to them (Sugarman, 1979, 72).

5 The Bureau of Reclamation, which built the ill-fated Teton Dam, allowed it to be filled rapidly, thus failing to provide sufficient time to monitor for the presence of leaks in a project constructed out of less than ideal soil. The Bureau did not heed the lesson of its Fontenelle Dam, where 10 years earlier massive leaks had also developed and caused a partial collapse (Shaw, 1977; Boffey, 1977).

These examples, and others to be given in later chapters, illustrate why it is not sufficient for engineers to rely on handbooks alone. Engineering, just like experimentation, demands practitioners who remain alert and well informed at every stage of a project's history.

Contrasts with Standard Experiments

To be sure, engineering differs in some respects from standard experimentation. Some of those very differences help to highlight the engineer's special

responsibilities. And exploring the differences can also aid our thinking about the moral responsibilities of all those engaged in engineering.

Experimental Control One great difference has to do with experimental control. In a standard experiment this involves the selection, at random, of members for two different groups. The members of one group receive the special, experimental treatment. Members of the other group, called the *control group*, do not receive that special treatment although they are subjected to the same environment as the first group in every other respect.

In engineering this is not the usual practice, unless the project is confined to laboratory experimentation, because the experimental subjects are humans out of the range of the experimenter's control. Indeed, clients and consumers exercise most of the control because it is they who choose the product or item they wish to use. This makes it impossible to obtain a random selection of participants from various groups. Nor can parallel control groups be established based on random sampling. Thus no careful study of the effects of changing variables on two or more comparison groups is possible, and one must simply work with the available historical and retrospective data about various groups that use the product.

This suggests that the view of engineering as a social experiment involves a somewhat extended usage of the concept of experimentation. Nevertheless, "engineering as social experimentation" should not be dismissed as a merely metaphorical notion. There are other fields where it is not uncommon to speak of experiments whose original purpose was not experimental in nature and that involve no control groups.

For example, social scientists monitor and collect data on differences and similarities between existing educational systems that were not initially set up as systematic experiments. In doing so they regard the current diversity of systems as constituting what has been called a "natural experiment" (as opposed to a deliberately initiated one) (Rivlin, 1970, 70). Similarly, we think that engineering can be appropriately viewed as just such a "natural experiment" using human subjects, despite the fact that most engineers do not currently consider it in that light.

Informed Consent Viewing engineering as an experiment on a societal scale places the focus where it should be: on the human beings affected by technology. For the experiment is performed on persons, not on inanimate objects. In this respect, albeit on a much larger scale, engineering closely parallels medical testing of new drugs and techniques on human subjects.

Society has recently come to recognize the primacy of the subject's safety and freedom of choice as to whether to participate in medical experiments. Ever since the revelations of prison and concentration camp horrors in the name of medicine, an increasing number of moral and legal safeguards have arisen to ensure that subjects in experiments participate on the basis of informed consent.

But while current medical practice has increasingly tended to accept as fundamental the subject's moral and legal rights to give informed consent before participating in an experiment, contemporary engineering practice is only beginning to recognize those rights. We believe that the problem of informed consent, which is so vital to the concept of a properly conducted experiment involving human subjects, should be the keystone in the interaction between engineers and the public. We are talking about the *lay public.* When a manufacturer sells a new device to a knowledgeable firm which has its own engineering staff, there is usually an agreement regarding the shared risks and benefits of trying out the technological innovation.

Informed consent is understood as including two main elements: knowledge and voluntariness. First, subjects should be given not only the information they request, but all the information which is needed for making a reasonable decision. Second, subjects must enter into the experiment without being subjected to force, fraud, or deception. Respect for the fundamental rights of dissenting minorities and compensation for harmful effects are taken for granted here.

The mere purchase of a product does not constitute informed consent, any more than does the act of showing up on the occasion of a medical examination. The public and clients must be given information about the practical risks and benefits of the product in terms they can understand. Supplying complete information about the product is neither necessary nor in most cases possible. In both medicine and engineering there may be an enormous gap between the experimenter's and the subject's understanding of the complexities of an experiment. But while this gap most likely cannot be closed, it should be possible to convey all pertinent information needed for making a reasonable decision on whether to participate or not.

We do not propose a proliferation of lengthy environmental impact reports. We favor the kind of sound advice a responsible physician gives a patient when prescribing a course of drug treatment that has possible side effects. The physician must search beyond the typical sales brochures from drug manufacturers for adequate information; hospital management must allow the physician the freedom to undertake different treatments for different patients, as each case may constitute a different "experiment" involving different circumstances; finally, the patient must be readied to receive the information.

Likewise, an engineer cannot succeed in providing essential information about a project or product unless there is cooperation by management and a receptivity on the part of those who should have the information. Management is often understandably reluctant to provide more information than current laws require, fearing disclosure to potential competitors and exposure to potential lawsuits. Moreover, it is possible that, paralleling the experience in medicine, clients or the public may not be interested in all of the relevant information about an engineering project, at least not until a crisis looms. It is important nevertheless that all avenues for disseminating such information be kept open and ready.

We note that the matter of informed consent is surfacing indirectly in the continuing debate over acceptable forms of energy. Representatives of the nuclear industry can be heard expressing their impatience with critics who worry about reactor malfunction while engaging in statistically more hazardous activities such as driving automobiles and smoking cigarettes. But what is being overlooked by those representatives is the common enough human readiness to accept risks voluntarily undertaken (as in daring sports), even while objecting to involuntary risks resulting from activities in which the individual is neither a direct participant nor a decision maker. In other words, we all prefer to be the subjects of our own experiments rather than those of somebody else. When it comes to approving a nearby oil-drilling platform or a nuclear plant, affected parties expect their consent to be sought no less than it is when a doctor contemplates surgery.

Prior consultation of the kind suggested can be effective. When Northern States Power Company (Minnesota) was planning a new power plant, it got in touch with local citizens and environmental groups before it committed large sums of money to preliminary design studies. The company was able to present convincing evidence regarding the need for a new plant and then suggested several sites. Citizen groups responded with a site proposal of their own. The latter was found acceptable by the company. Thus informed consent was sought from and voluntarily given by those the project affected, and the acrimonious and protracted battle so common in other cases where a company has already invested heavily in decisions based on engineering studies alone was avoided (Borrelli, 36–39). Note that the utility company interacted with groups that could serve as proxy for various segments of the ratepaying public. Obviously it would have been difficult to involve the ratepayers individually.

We endorse a broad notion of informed consent, or what some would call *valid consent* (Culver and Gert), defined by the following conditions:

1 The consent was given voluntarily.

2 The consent was based on the information that a rational person would want, together with any other information requested, presented to them in understandable form.

3 The consenter was competent (not too young or mentally ill, for instance) to process the information and make rational decisions.

We suggest two requirements for situations in which the subject cannot be readily identified as an individual:

4 Information that a rational person would need, stated in understandable form, has been widely disseminated.

5 The subject's consent was offered in proxy by a group that collectively represents many subjects of like interests, concerns, and exposure to risk.

Knowledge Gained

Scientific experiments are conducted to gain new knowledge, while "engineering projects are experiments that are not necessarily designed to produce

very much knowledge," according to a valuable interpretation of our paradigm by Broome (1987). When we carry out an engineering activity as if it were an experiment, we are primarily preparing ourselves for unexpected outcomes. The best outcome in this sense is one which tells us nothing new but merely affirms that we are right about something. Unexpected outcomes send us on a search for new knowledge—possibly involving an experiment of the first (scientific) type. For the purposes of our model the distinction is not vital because we are concerned about the manner in which the experiment is conducted, such as that valid consent of human subjects is sought, safety measures are taken, and means exist for terminating the experiment at any time and providing all participants a safe exit.

Study Questions

1 On June 5, 1976, Idaho's Teton Dam collapsed, killing eleven people and causing $400 million in damage. Drawing upon the concept of engineering as social experimentation, discuss the following facts uncovered by the General Accounting Office and reported in the press.
   a Because of the designers' confidence in the basic design of Teton Dam, it was believed that no significant water seepage would occur. Thus sufficient instrumentation to detect water erosion was not installed.
   b Significant information suggesting the possibility of water seepage was acquired at the dam site 6 weeks before the collapse. It was sent through routine channels from the project supervisors to the designers, and arrived at the designers the day after the collapse.
   c During the important stage of filling the reservoir, there was no around-the-clock observation of the dam. As a result the leak was detected only 5 hours before the collapse. Even then the main outlet could not be opened to prevent the collapse because a contractor was behind schedule in completing the outlet structure (Shaw, 1977, 3; Boffee, 1977, 270–272).
2 The University of California uses tax dollars to develop farm machinery such as tomato, lettuce, melon harvesters, and fruit tree shakers. Such machinery reduces the need for farm labor and raises farm productivity. It definitely benefits the growers. It is also said to benefit all of society. Farm workers, however, claim that replacing an adequate and willing work force with machines will generate social costs not offset by higher productivity. Among the costs they cite are the need to retrain farm workers for other jobs and the loss of small farms. Discuss if and how continuing farm mechanization may be viewed as an experiment.
3 Apply the social experimentation model to the DC-10 case described in Chap. 2. Specifically, in order to facilitate informed consent concerning dangers entailed by the plane's design, should Dan Applegate have been allowed to convey information to public representatives (in government or consumer groups) or directly (via newspapers) to the public who must decide whether to fly on DC-10 airplanes?
4 Models often influence thinking by effectively organizing and guiding reflection and crystallizing attitudes. Yet they usually have limitations and can themselves be misleading to some degree. Write a short essay in which you critically assess the strengths and weaknesses you see in the social experimentation model.

   One possible criticism you might consider is whether the model focuses too much on the creation of new products, whereas a great deal of engineering in-

volves the routine application of results from past work and projects. Another point to consider is how informed consent is to be measured in situations where groups are involved, as in the construction of a nuclear power plant near a community of people having mixed views about the advisability of constructing the plant.

5 Debates over responsibility for safety in regard to technological products often turn on whether the consumer should be considered mainly responsible ("buyer beware") or the manufacturer ("seller beware"). How might an emphasis on the idea of informed consent influence thinking about this question?

6 In the following passage from *A Nation of Guinea Pigs*, Marshall Shapo applies the concept of experimentation to the marketing of drugs. Comment on parallels and dissimilarities you see between the moral aspects of social experimentation in engineering and in drug marketing.

> . . . experimentation is a label which connotes an attempt to solve problems in a fresh and novel way, using the subjects of the attempt as means to gather information. The image that the term conveys in the context of hazards involving products and processes tends to be a laboratory image. But much experimentation goes beyond the laboratory. In the process of testing and marketing new drugs, after procedures first limited to testing for toxicity and pharmacological effects, it takes place with increasingly large groups of patients in clinical trials. And although we do not conventionally attach the label "experimental" to the general marketing of products, it is clear that widespread distribution in fact involves a continuous process of experimentation. Especially with goods that are scientifically complex, the information-collecting goal of the experimenter is never attained in the formally investigational stages of the process. Some hazards may become apparent only after the products are used by millions of people, and over extended periods of time (Shapo, 1979, 30).

7 Engineering and medical practice are intimately linked in medical engineering. Its products range from artificial limbs and organs to heart pacers and x-ray machines. Its engineers and medical experts are experimenters with excellent track records, but failures do occur. For example, the State University of New York at Albany admitted that its psychology department had conducted electroshock experiments on patients who were not given fair explanations of risks and whose consent had not been obtained. The machine itself was unsafe (R. J. Smith, 1977). Discuss the ethical implications of this case.

8 "On Being One's Own Rabbit" is the title of an essay by J. B. Haldin, who conducted many risky medical experiments on his own body (quoted in Mullan, 1987). Seek examples of engineers and inventors who served as their own subjects and discuss to what extent such practice is desirable or not. (Example: Wright Brothers)

9 *"Primum non nocere"* ("Above all, do not harm") is an admonition to medical students and practitioners. What should engineers do when hired to carry out tasks they feel might cause harm? Are clients not entitled to engineering services in the same way that we insist on legal services being available to everyone, including crooks? In certain restricted cases it might be morally justifiable for engineers to proceed with the requested task. Baum (1980) made the concept of informed consent central to thinking about engineering ethics in connection with such circumstances. Describe a real or hypothetical situation where engineer, client, and affected parties might disagree and another case where they might agree.

ENGINEERS AS RESPONSIBLE EXPERIMENTERS

What are the responsibilities of engineers to society? Viewing engineering as social experimentation does not by itself answer this question. For while engineers are the main technical enablers or facilitators, they are far from being the sole experimenters. Their responsibility is shared with management, the public, and others. Yet their expertise places them in a unique position to monitor projects, to identify risks, and to provide clients and the public with the information needed to make reasonable decisions.

The detailed content of engineers' responsibilities, in the sense of obligations, will be explored throughout the remainder of this book. At present we are interested in another of the senses of "responsibility" distinguished in Chap. 2. We want to know what is involved in displaying the virtue of being a responsible person while acting as an engineer. From the perspective of engineering as social experimentation, what are the general features of morally responsible engineers?

At least four elements are pertinent: a conscientious commitment to live by moral values, a comprehensive perspective, autonomy, and accountability (Haydon, 1978, 50–53). Or, stated in greater detail as applied to engineering projects conceived as social experiments:

1 A primary obligation to protect the safety of and respect the right of consent of human subjects
2 A constant awareness of the experimental nature of any project, imaginative forecasting of its possible side effects, and a reasonable effort to monitor them
3 Autonomous, personal involvement in all steps of a project
4 Accepting accountability for the results of a project

It is implied in the foregoing that engineers should also display technical competence and other attributes of professionalism. Inclusion of these four requirements as part of engineering practice would then earmark a definite "style" of engineering. In elaborating upon this style, we will note some of the contemporary threats to it.

Conscientiousness

People act responsibly to the extent that they conscientiously commit themselves to live according to moral values. But moving beyond this truism leads immediately to controversy over the precise nature of those values. In Chap. 1 we adopted the minimal thesis that moral values transcend a consuming preoccupation with a narrowly conceived self-interest. Accordingly, individuals who think solely of their own good to the exclusion of the good of others are not moral agents. By *conscientious* moral commitment is meant a sensitivity to the full range of moral values and responsibilities that are relevant to a given situation, and the willingness to develop the skill and expend the effort needed to reach the best balance possible among those considerations.

The contemporary working conditions of engineers tend to narrow moral vision solely to the obligations that accompany employee status. As stated earlier, some 90 percent of engineers are salaried employees, most of whom work within large bureaucracies under great pressure to function smoothly within the organization. There are obvious benefits in terms of prudential self-interest and concern for one's family that make it easy to emphasize as primary the obligations to one's employer. Gradually the minimal negative duties, such as not falsifying data, not violating patent rights, and not breaching confidentiality, may come to be viewed as the full extent of moral aspiration.

Conceiving engineering as social experimentation restores the vision of engineers as guardians of the public interest, whose professional duty it is to guard the welfare and safety of those affected by engineering projects. And this helps to ensure that such safety and welfare will not be disregarded in the quest for new knowledge, the rush for profits, a narrow adherence to rules, or a concern over benefits for the many that ignores harm to the few.

The role of social guardian should not suggest that engineers force, paternalistically, their own views of the social good upon society. For, as with medical experimentation on humans, the social experimentation involved in engineering should be restricted by the participant's consent—voluntary and informed consent.

Relevant Information

Conscientiousness is blind without relevant factual information. Hence showing moral concern involves a commitment to obtain and properly assess all available information pertinent to meeting one's moral obligations. This means, as a first step, fully grasping the *context* of one's work which makes it *count* as an activity having a moral import.

For example, there is nothing wrong in itself with being concerned to design a good heat exchanger. But if I ignore the fact that the heat exchanger will be used as part of a still involved in the manufacture of a potent, illegal hallucinogen, I am showing a lack of moral concern. It is this requirement that one be aware of the wider implications of one's work which makes participation in, say, a design project for a superweapon morally problematic—and which makes it sometimes convenient for engineers self-deceivingly to ignore the wider context of their activities, a context that may rest uneasily with an active conscience.

Another way of blurring the context of one's work results from the ever increasing specialization and division of labor which makes it easy to think of someone else in the organization as responsible for what otherwise might be a bothersome personal problem. For example, a company may produce items with obsolescence built into them, or the items might promote unnecessary energy usage. It is easy to place the burden on the sales department: "Let *them* inform the customers—if the customers ask." It may be natural to thus rationalize one's neglect of safety or cost considerations, but it shows no moral concern.

These ways of losing perspective on the nature of one's work also hinder acquiring a full perspective along a second dimension of factual information: the *consequences* of what one does. And so while regarding engineering as social experimentation points out the importance of context, it also urges the engineer to view his or her specialized activities in a project as part of a larger whole having a social impact—an impact that may involve a variety of unintended effects. Accordingly, it emphasizes the need for wide training in disciplines related to engineering and its results, as well as the need for a constant effort to imaginatively foresee dangers.

It might be said that the goal is to practice what Chauncey Starr once called "defensive engineering." Or perhaps more fundamental is the concept of "preventive technology" as described by Ruth Davis, who could have addressed the following lines equally well to engineers as she did to scientists and physicians:

> The solution to the problem is not in successive cures to successive science-caused problems; it is in their prevention. Unfortunately, cures for scientific ills are generally more interesting to scientists than is the prevention of those ills. We have the unhappy history of the medical community to show us the difficulties associated with trying to establish preventive medicine as a specialty.
>
> Scientists probably had more fun developing scientific defenses against nuclear weapons (that is, cures) than they would have had practicing preventive nuclear science during the development of the atomic bomb. Computer scientists find it more attractive to develop technological safeguards, after the fact, to prevent invasions of privacy associated with computer data banks than to develop good information practices along with the computer systems.
>
> However, it now seems quite clear that public patience with the cure always following after the ill has worn thin. The public wants to see some preventive measures taken. Indeed, individuals have taken what can be called preventive technology into their own hands. We have seen the public in action in this way in its handling of the supersonic transport issue and its reaction toward siting of nuclear power plants. This is the reactive mode of practicing preventive technology, and it hinges on public recognition that technology is fallible (Davis, 1975, 213).

No amount of disciplined and imaginative foresight, however, can serve to anticipate all dangers. Because engineering projects are inherently experimental in nature, it is crucial for them to be monitored on an ongoing basis from the time they are put into effect. While individual practitioners cannot privately conduct full-blown environmental and social impact studies, they can choose to make the extra effort needed to keep in touch with the course of a project after it has officially left their hands. This is a mark of *personal* identification with one's work, a notion that leads to the next aspect of moral responsibility.

Moral Autonomy

People are morally autonomous when their moral conduct and principles of action are their *own*, in a special sense deriving from Kant. That, is, moral

beliefs and attitudes must be held on the basis of critical reflection rather than merely through passive adoption of the particular conventions of one's society, church, or profession. This is often what is meant by "authenticity" in one's commitment to moral values.

Those beliefs and attitudes, moreover, must be integrated into the core of an individual's personality in a manner that leads to committed action. They cannot be agreed to abstractly and formally and adhered to merely verbally. Thus, just as one's principles are not passively imbibed from others when one is morally autonomous, so too one's actions are not treated as something alien and apart from oneself.

It is a comfortable illusion to think that in working for an employer, and thereby performing acts directly serving a company's interests, one is no longer morally and personally identified with one's actions. Selling one's labor and skills may make it seem that one has thereby disowned and forfeited power over one's actions (Lachs, 1978, 201–213).

Viewing engineering as social experimentation can help one overcome this tendency and can help restore a sense of autonomous participation in one's work. As an experimenter, an engineer is exercising the sophisticated training that forms the core of his or her identity as a professional. Moreover, viewing an engineering project as an experiment that can result in unknown consequences should help inspire a critical and questioning attitude about the adequacy of current economic and safety standards. This also can lead to a greater sense of personal involvement with one's work.

The attitude of management plays a decisive role in how much moral autonomy engineers feel they have. It would be in the long-term interest of a high-technology firm to grant its engineers a great deal of latitude in exercising their professional judgment on moral issues relevant to their jobs (and, indeed, on, technical issues as well). But the yardsticks by which a manager's performance is judged on a quarterly or yearly basis most often militate against this. This is particularly true in our age of conglomerates, when near-term profitability is more important than consistent quality and long-term retention of satisfied customers.

In government-sponsored projects it is frequently a deadline which becomes the ruling factor, along with fears of interagency or foreign competition. Tight schedules contributed to the loss of the U.S. space shuttle *Challenger* as we shall see later.

Accordingly engineers are compelled to look to their professional societies and other outside organizations for moral support. Yet it is no exaggeration to claim that the blue-collar worker with union backing has greater leverage at present in exercising moral autonomy than do many employed professionals. A steel plant worker, for instance, who refused to dump oil into a river in an unauthorized manner was threatened with dismissal, but his union saw to it that the threat was never carried out (Nader, 1972, 189). Or take the case of the automobile plant inspector who repeatedly warned his supervisors about poorly welded panels which allowed carbon monoxide from the exhaust to leak into the cab. Receiving no satisfactory response from the company, he

blew the whistle. The company wanted to fire him, but pressure from the union allowed him to keep his job. (The union, however, did not concern itself with the safety issue. It was probably as surprised as the company by the number of eventual fatalities traceable to the defect, the recall order those deaths necessitated, and the tremendous financial loss ultimately incurred by the company.) (Nader, 1972, 75–89)

Professional societies, originally organized as learned societies dedicated to the exchange of technical information, lack comparable power to protect their members, although most engineers have no other group to rely on for such protection. Only now is the need for moral and legal support of members in the exercise of their professional obligations being recognized by those societies. Unger (1987) describes how engineering societies can proceed, even in the face of difficulties such as litigation.

Accountability

Finally, responsible people accept moral responsibility for their actions. Too often "accountable" is understood in the overly narrow sense of being culpable and blameworthy for misdeeds. But the term more properly refers to the general disposition of being willing to submit one's actions to moral scrutiny and be open and responsive to the assessments of others. It involves a willingness to present morally cogent reasons for one's conduct when called upon to do so in appropriate circumstances.

Submission to an employer's authority, or any authority for that matter, creates in many people a narrowed sense of accountability for the consequences of their actions. This was documented by some famous experiments conducted by Stanley Milgram during the 1960s (Milgram, 1974). Subjects would come to a laboratory believing they were to participate in a memory and learning test. In one variation two other people were involved, the "experimenter" and the "learner." The experimenter was regarded by the subject as an authority figure, representing the scientific community. He or she would give the subject orders to administer electric shocks to the "learner" whenever the latter failed in the memory test. The subject was told the shocks were to be increased in magnitude with each memory failure. All this, however, was a deception—a "setup." There were no real shocks and the apparent "learner" and the "experimenter" were merely acting parts in a ruse designed to see how far the unknowing experimental subject was willing to go in following orders from an authority figure.

The results were astounding. When the subjects were placed in an adjoining room separated from the "learner" by a shaded glass window, over half were willing to follow orders to the full extent: giving the maximum electric jolt of 450 volts. This was in spite of seeing the "learner," who was strapped in a chair, writhing in (apparent) agony. The same results occurred when the subjects were allowed to hear the (apparently) pained screams and protests of the "learner," screams and protests which became intense from 130 volts on. There was a striking difference, however, when subjects were placed in

the same room within touching distance of the "learner." Then the number of subjects willing to continue to the maximum shock dropped by one-half.

Milgram explained these results by citing a strong psychological tendency in people to be willing to abandon personal accountability when placed under authority. He saw his subjects ascribing all initiative, and thereby all accountability, to what they viewed as legitimate authority. And he noted that the closer the physical proximity, the more difficult it becomes to divest oneself of personal accountability.

The divorce between causal influence and moral accountability is common in business and the professions, and engineering is no exception. Such a psychological schism is encouraged by several prominent features of contemporary engineering practice.

First, large-scale engineering projects involve fragmentation of work. Each person makes only a small contribution to something much vaster. Moreover, the final product is often physically removed from one's immediate workplace, creating the kind of "distancing" that Milgram identified as encouraging a lessened sense of personal accountability.

Second, corresponding to the fragmentation of work is a vast diffusion of accountability within large institutions. The often massive bureaucracies within which most engineers work are designed to diffuse and delimit areas of personal accountability within hierarchies of authority.

Third, there is frequently pressure to move on to a new project before the current one has been operating long enough to be observed carefully. This promotes a sense of being accountable only for meeting schedules.

Fourth, the contagion of malpractice suits currently afflicting the medical profession is carrying over into engineering. With this comes a crippling preoccupation with legalities, a preoccupation which makes one wary of becoming morally involved in matters beyond one's strictly defined institutional role.

We do not mean to underestimate the very real difficulties these conditions pose for engineers who seek to act as morally accountable people on their jobs. Much less do we wish to say engineers are blameworthy for all the bad side effects of the projects they work on, even though they partially cause those effects simply by working on the projects. That would be to confuse accountability with blameworthiness, and also to confuse causal responsibility with moral responsibility. But we do claim that engineers who endorse the perspective of engineering as a social experiment will find it more difficult to divorce themselves psychologically from personal responsibility for their work. Such an attitude will deepen their awareness of how engineers daily cooperate in a risky enterprise in which they exercise their personal expertise toward goals they are especially qualified to attain, and for which they are also accountable.

Study Questions

1 A common excuse for carrying out a morally questionable project is, "If I don't do it somebody else will." This rationale may be tempting for engineers who typically

work in situations where someone else might be ready to replace them on a project. Do you view it as a legitimate excuse for engaging in projects which might be unethical? (In your answer, comment upon the concept of responsible conduct developed in this section.)

2 Another commonly used phrase, "I only work here," implies that one is not personally accountable for the company rules since one does not make them. It also suggests that one wishes to restrict one's area of responsibility within tight bounds as defined by those rules (Lachs, 1978, 201–213). In light of the discussion in this section, respond to the potential implications of this phrase and the attitude represented by it when exhibited by engineers.

3 You have been asked to design an electronic vote counter for a legislative body. You have no difficulty with the physical features of the machine, but you begin to ask yourself some questions. If heretofore all votes, except for secret ballots, were by a show of hands, should a display board be provided indicating each individual vote? Or would total tallies be sufficient, thereby assuring anonymity of voting on each occasion? What would be the implication of each option in terms of respecting the public's right to know? How much need you worry about unauthorized tampering with such a machine? Describe to what extent the model of social experimentation can be applied to the introduction of the vote counter. (For a short report on the West German parliament's reluctance to put a vote counter to use in 1971, see the *Los Angeles Times* article by Joe Alex Morris, Jr., cited in the Bibliography.)

4 Threats to a sense of personal responsibility are neither unique to nor more acute for engineers than they are for others involved with engineering and its results. The reason is that, in general, *public* accountability also tends to lessen as professional roles become narrowly differentiated. With this in mind, critique each of the remarks made in the following dialogue. Is the remark true, or partially true? What needs to be added to make it accurate?

Engineer: My responsibility is to receive directives and to create products within specifications set by others. The decision about what products to make and their general specifications are economic in nature and made by management.

Scientist: My responsibility is to gain knowledge. How the knowledge is applied is an economic decision made by management, or else a political decision made by elected representatives in government.

Manager: My responsibility is solely to make profits for stockholders.

Stockholder: I invest my money for the purpose of making a profit. It is up to managers to make decisions about the directions of technological development.

Consumer: My responsibility is to my family. Government should make sure corporations do not harm me with dangerous products, harmful side effects of technology, or dishonest claims.

Government regulator: By current reckoning, government has strangled the economy through overregulation of business. Accordingly at present on my job, especially given decreasing budget allotments, I must back off from the idea that business should be policed, and urge corporations to assume greater public responsibility.

5 Cancer therapy machines were discarded at dump sites in Juarez, Mexico (R.J. Smith, 1984) , and Goiânia, Brazil (L. Roberts, 1987). The radioactive isotopes, removed from their canisters, exposed many people. At least one child died. Discuss

the responsibility of the manufacturers' and hospitals' engineers for safe disposal of such apparatus. Is this part of the monitoring function set forth in the engineering as experiment paradigm?

6 Is this a true experiment, wishful thinking, or a scam? The Cryonics movement believes in keeping fresh corpses frozen, with blood replaced by glycol antifreeze, until advances in medicine can cure the original cause of death. Then the body is to be unfrozen, the cure applied, and the patient returned to life. Several bodies are kept in cryogenic facilities around the United States, along with several heads, which are kept for future attachment to cloned bodies. Research the case and discuss how it fits the experimentation model. Here are some references to get you started: issues of *Omni* (October 1986) and *Health* (March 1987); the book *Freezing Point* by L. Kavaler (1970).

THE *CHALLENGER* CASE

Several months before the destruction of the *Challenger*, NASA historian Alex Roland wrote the following in a critical piece about the space shuttle program:

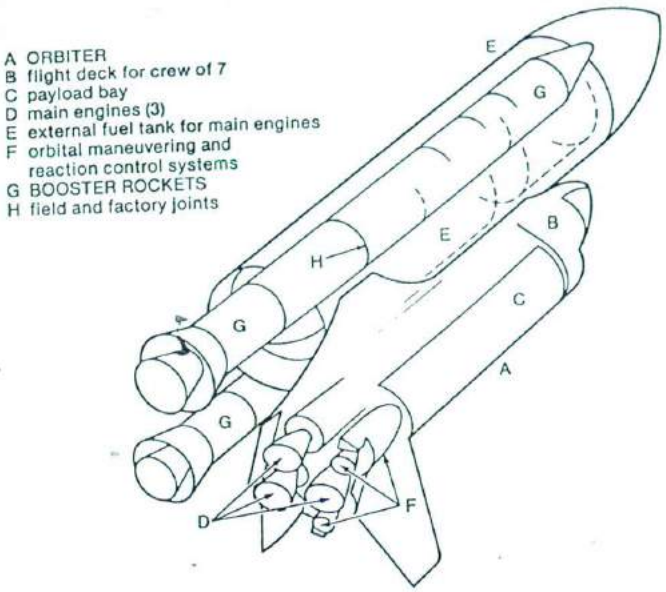
> The American taxpayer bet about $14 billion on the shuttle. NASA bet its reputation. The Air Force bet its reconnaissance capability. The astronauts bet their lives. We all took a chance.
>
> When John Young and Robert Crippen climbed aboard the orbiter *Columbia* on April 12, 1981 for the first shuttle launch, they took a bigger chance than any astronaut before them. Never had Americans been asked to go on a launch vehicle's maiden voyage. Never had astronauts ridden solid propellant rockets. Never had Americans depended on an engine untested in flight (Roland, 1985).

Most of Roland's criticism was directed at the economic and political side of what was supposed to become a self-supporting operation but never gave any indication of being able to reach that goal. Without a national consensus to back it, the shuttle program became a victim of year by year funding politics (Logsdon, 1986).

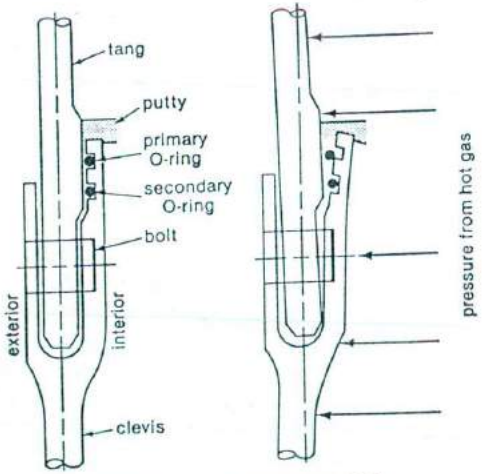
The *Columbia* and its sister ships, the *Challenger* and *Discovery*, are delta-wing craft with a huge payload bay. Early, sleek designs had to be abandoned to satisfy U.S. Air Force requirements when the latter was ordered to use the NASA shuttle instead of its own expendable rockets for launching satellites and other missions. As shown in Fig. 3-1 each orbiter has three main engines fueled by several million pounds of liquid hydrogen; the fuel is carried in an immense, external, divided fuel tank, which is jettisoned when empty. During lift-off the main engines fire for about 8.5 minutes, although during the first 2 minutes of the launch much of the thrust is provided by two booster rockets. These are of the solid-fuel type, each burning a 1-million-pound load of a mixture of aluminum, potassium chloride, and iron oxide.

The casing of each booster rocket is about 150 feet long and 12 feet in diameter. It consists of cylindrical segments which are assembled at the launch site. The four field joints use seals composed of pairs of O-rings made of vulcanized rubber. The O-rings work in conjunction with a putty barrier of zinc chromide.

The shuttle flights were successful, though not as frequent as had been



a) Space Shuttle



Challenger BEFORE IGNITION AFTER IGNITION (movement shown is exaggerated)

b) Cross-section of Field Joint

FIGURE 3-1
Space shuttle *Challenger*.

hoped. NASA tried hard to portray the shuttle program as an operational system that could pay for itself. Some Reagan administration officials had even suggested that the operations be turned over to an airline. Aerospace engineers intimately involved in designing, manufacturing, assembling, testing, and operating the shuttle still regarded it as an experimental undertaking in 1986. These engineers were employees of manufacturers, such as Rockwell International (orbiter and main rocket) and Morton-Thiokol (booster rockets), or they worked for NASA at one of its several centers: Marshall Space Flight Center, Huntsville, Alabama (responsible for the propulsion system); Kennedy Space Center, Cape Kennedy, Florida (launch operations); Johnson Space Center, Houston, Texas (flight control); and the office of the Chief Engineer, Washington, D.C. (overall responsibility for safety, among other duties).

After embarrassing delays, *Challenger*'s first flight for 1986 was set for Tuesday morning, January 28. But Allan J. McDonald, who represented Morton-Thiokol at Cape Kennedy, was worried about the freezing temperatures predicted for the night. As his company's director of the solid-rocket booster project he knew of difficulties that had been experienced with the field joints on a previous cold-weather launch when the temperature had been mild compared to what was forecast. He therefore arranged a teleconference so that NASA engineers could confer with Morton-Thiokol engineers at their plant in Utah.

Arnold Thompson and Roger Boisjoly, two seal experts at Morton-Thiokol, explained to their own colleagues and managers as well as the NASA representatives how upon launch the booster rocket walls bulge and the combustion gases can blow past one or even both of the O-rings which make up the field joints (see Fig. 3-1). The rings char and erode, as had been observed on many previous flights. In cold weather the problem is aggravated because the rings and the putty packing are less pliable then.

The engineering managers, Bob Lund (V.P. of engineering) and Joe Kilminster (V.P. for booster rockets), agreed that there was a problem with safety. The team from Marshall Space Flight Center was incredulous. Since the specifications called for an operating temperature of the solid fuel prior to combustion of 40 to 90 degrees Fahrenheit, one could surely allow lower or higher outdoor temperatures, notwithstanding Boisjoly's testimony and recommendation that no launch should occur at less than 53 degrees. They were clearly annoyed at facing yet another postponement.

Top executives of Morton-Thiokol were also sitting in on the teleconference. Their concern was the image of the company, which was in the process of negotiating a renewal of the booster rocket contract with NASA. During a recess Senior Vice President Jerry Mason turned to Bob Lund and told him "to take off your engineering hat and put on your management hat." It was a subsequent vote (of the managers only) that produced the company's official finding that the seals could not be shown to be unsafe. The engineers' judgment was not considered sufficiently weighty. At Cape Kennedy, Allan

McDonald refused to sign the formal recommendation to launch; Joe Kilminster had to do that.

Accounts of the *Challenger* disaster (McConnell, 1987; Rogers Commission Report, 1986) tell of the cold Tuesday morning, the high seas which forced the recovery ships to seek coastal shelter, the ice at the launch site, and the concern expressed by Rockwell engineers that the ice might shatter and hit the orbiter or rocket casings. The inability of these engineers to prove that the lift-off would be unsafe was taken by NASA as an approval by Rockwell to launch.

The countdown ended at 11:38 A.M. The temperature had risen to 36 degrees. As the rockets carrying *Challenger* rose from the ground, cameras recorded puffs of smoke which emanated from one of the field joints on the right booster rocket. Soon these turned into a flame which hit the external fuel tank and a strut holding the booster rocket. The hydrogen in the tank caught fire, the booster rocket broke loose, smashed into *Challenger*'s wing, then into the external fuel tank. At 76 seconds into the flight, by the time *Challenger* and its rockets had reached 50,000 feet, it was totally engulfed in a fireball. The crew cabin separated and fell into the ocean, killing all aboard: mission commander Francis (Dick) Scobee; pilot Michael Smith; mission specialists Gregory Jarvis, Ronald McNair, Ellison Onizuka, Judith Resnick; "teacher in space" Christa MacAuliffe.

President Reagan was to give his State of the Union message later that day. He had to change the tone of his prepared remarks on the shuttle flight and its first civilian passenger.

Safety Issues

Unlike the three-stage rockets which carried astronauts to the moon, the space shuttle could be involved in a simultaneous (inadvertent) ignition of all fuel carried aloft. An explosion close to the ground can have catastrophic effects. The crew has no escape mechanism, although McDonnell-Douglas, in a losing shuttle proposal, had provided an abort module with its own thruster. It would have allowed the separation of the orbiter, triggered (among other events) by a field-joint leak. But such a safety measure was rejected as too expensive because of an accompanying reduction in payload.

Working with such constraints, why was safe *operation* not stressed more? First of all we must remember that the shuttle program was indeed still a truly experimental and research undertaking. Next, it is quite clear that the members of the crews knew that they were embarking on dangerous missions. But it has also been revealed that the *Challenger* astronauts were not informed of particular problems such as the field joints. They were not asked for their consent to be launched under circumstances which experienced engineers had claimed to be unsafe.

The reason for the rather cavalier attitude toward safety is revealed in the way NASA assessed the system's reliability. For instance, recovered booster rocket casings had indicated that the field-joint seals had been damaged in many of the earlier flights. The waivers necessary to proceed with launches

had become mere gestures. Richard Feynman made the following observations as a member of the Presidential Commission on the Space Shuttle *Challenger* Accident (called the Rogers Commission after its chairman):

> I read all of these [NASA flight readiness] reviews and they agonize whether they can go even though they had some blow-by in the seal or they had a cracked blade in the pump of one of the engines,...and they decide "yes." Then it flies and nothing happens. Then it is suggested...that the risk is no longer so high. For the next flight we can lower our standards a little bit because we got away with it last time....It is a kind of Russian roulette (Rogers Commission Report, 1986).

Since the early days of unmanned space flight, about 1 in every 25 solid-fuel rocket boosters has failed. Given improvements over the years, Feynman thought that 1 in every 50 to 100 might be a reasonable estimate now (Marshall, 1986). Yet NASA counts on only 1 crash in every 100,000 launches. Queried about these figures, NASA Chief Engineer Milton Silveira answered: "We don't use that number as a management tool. We know that the probability of failure is always sitting there..." (Marshall, 1986). So where was this number used? In a risk analysis needed by the Department of Energy to assure everyone that it would be safe to use small atomic reactors as power sources on deep-space probes and to carry both aloft on a space shuttle. As luck would have it, *Challenger* was not to carry the 47.6 pounds of lethal plutonium-238 until its next mission with the *Galileo* probe on board (Grossman, 1986).

Another area of concern was NASA's unwillingness to wait out risky weather. When serving as weather observer, astronaut John Young was dismayed to find his recommendations to postpone launches disregarded several times. Things had not changed much by March 26, 1987, when NASA neglected to heed its monitoring devices for electric storm conditions, launched a Navy communications satellite atop an Atlas-Centaur rocket, and had to destroy the $160 million system when it veered off course after being hit by lightning. The monitors had been installed after a similar event involving an Apollo command module 18 years before had nearly aborted a trip to the moon (Marshall, 1987). Weather, incidentally, could be held partially responsible for the shuttle disaster because a strong wind shear may have contributed to the rupturing of the weakened O-rings (Bell, 1987).

Veteran astronauts were also dismayed at NASA management's decision to land at Cape Kennedy as often as possible despite its unfavorable landing conditions including strong crosswinds and changeable weather. The alternative, Edwards Air Force Base in California, is a better landing place but necessitates a piggyback ride for the shuttle on a Boeing 747 home to Florida. This costs time and money.

In 1982 Albert Flores conducted a study of safety concerns at the Johnson Space Center. He found its engineers to be strongly committed to safety in all aspects of design. When they were asked how managers might further improve safety awareness, there were few concrete suggestions but many comments on how safety concerns were ignored or negatively impacted by man

agement. One engineer was quoted as saying, "A small amount of professional safety effort and upper management support can cause a quantum safety improvement with little expense" (Flores, 1982, 79). This points to the important role of management in building a strong sense of responsibility for safety first and to schedules second.

The space shuttle's field joints are designated to be of criticality 1, which means there is no backup. Therefore a leaky field joint will result in failure of the mission and loss of life. There are 700 items of criticality 1 on the shuttle. A problem with any one of them should have been cause enough to do more than launch more shuttles without modification while working on a better system. Improved seal designs had already been developed, but the new rockets would not have been ready for some time. In the meantime the old booster rockets should have been recalled.

At Morton-Thiokol, Roger Boisjoly's personal concern had been heightened by his memory of the DC-10 crash over Paris. That accident had shown him how known defects can be disregarded in a complex organization. For this reason he had started a journal in which he recorded all events associated with the seals (Whitbeck, 1987). But like Dan Applegate in the DC-10 case he probably did not feel that he had the kind of professional backing which would allow him to go beyond his organization directly to the astronauts.

In several respects the ethical issues in the Challenger case resemble those of the DC-10 case. Concern for safety gave way to institutional posturing. Danger signals did not go beyond Convair and Douglas Aircraft in the DC-10 case; they did not go beyond Morton-Thiokol and Marshall Space Flight Center in the *Challenger* case. No effective recall was instituted. There were concerned engineers who spoke out, but ultimately they felt it only proper to submit to management decisions.

The major difference between the cases is found in the late-hour teleconference which Allan McDonald had arranged from the *Challenger* launch site to get knowledgeable engineers to discuss the seal problem from a technical viewpoint. (No similar conference between engineers from different organizations took place in the DC-10 case.) This tense conference did not involve lengthy discussions of ethics, but it revealed the virtues (or lack thereof) which allow us to distinguish between the "right stuff" and the "wrong stuff." This is well described in the following letter to the *Los Angeles Times* by an aerospace engineer.

> In Paul Conrad's cartoon (Feb. 27, 1986), "Autopsy of a Catastrophe," a drawing of the space shuttle *Challenger* is labeled with words like "MONEY," "SCHEDULE," etc. Forty years experience as an engineer in the aerospace industry leads me to believe that Conrad has (uncharacteristically) defused the issue.
>
> He could have used one word, "arrogance." The arrogance that prompts higher-level decision makers to pretend that factors other than engineering judgement should influence flight safety decisions and, more important, the arrogance that rationalizes overruling the engineering judgement of engineers close to the problem by those whose expertise is naive and superficial by comparison.
>
> The flaw is not in the decision-making process; it is in the decision-making

mentality. Consequently it would be of little value to move engineering decisions to a higher level, as has been contemplated by members of the presidential investigating commission" (Moeller, 1986).

Included, surely, is the arrogance of those who reversed NASA's (paraphrased) motto "Don't fly if it cannot be shown to be safe" to "Fly unless it can be shown not to be safe."

At Morton-Thiokol some of the vice presidents in the space division have been demoted. The engineers who were outspoken at the prelaunch teleconference and again before the Rogers Commission kept their jobs at the company because of congressional pressure, but their jobs are of a pro forma nature. In a speech to engineering students at the Massachussetts Institute of Technology a year after the *Challenger* disaster, Roger Boisjoly said: "I have been asked by some if I would testify again if I knew in advance of the potential consequences to me and my career. My answer is always an immediate yes. I couldn't live with any self-respect if I tailored my actions based upon potential personal consequences as a result of my honorable actions..." (Boisjoly, 1987).

Today NASA has a policy which allows aerospace workers with concerns to report them anonymously to the Batelle Memorial Institute in Columbus, Ohio, but open disagreement still invites harrassment (Magnuson, 1988).

Study Questions

1 Read more detailed accounts of the Challenger disaster and then examine if and how the principal actors in this tragedy behaved as responsible experimenters within the framework of the engineering as experimentation model.

2 Chairman Rogers asked Bob Lund: "Why did you change your decision [that the seals would not hold up] when you changed hats?" What might motivate you, as a midlevel manager, to go along with top management when told to "take off your engineering hat and put on your management hat"?

3 Under what conditions would you say it is safe to launch a shuttle without an escape mechanism for the crew?

4 Discuss the role of the astronauts in shuttle safety. To what extent should they (or at least the orbiter commanders) have involved themselves more actively in looking for safety defects in design or operation?

5 Consider the following actions or recommendations and suggest a plan of action to bring about safer designs and operations in a complex organization.

   a Lawrence Mulloy represented Marshall Space Flight Center at Cape Kennedy. He did not tell Arnold Aldrich from the National Space Transportation Program at Johnson Space Center about the discussions regarding the field-joint seals even though Aldrich had the responsibility of clearing Challenger for launch. Why? Because the seals were "a Level III issue," and Mulloy was at Level III, while Aldrich was at a higher level (Level II) which ought not to be bothered with such details.

   b The Rogers Commission recommended that an independent safety organization directly responsible to the NASA administrator be established. At the end of the *Challenger* case study we mentioned that an anonymous reporting scheme now exists for aerospace industry employees working on NASA projects.

c Tom Peters advises managers to "involve everyone in everything. . . . Boldly assert that there is no limit to what the average person can accomplish if thoroughly involved" (Peters, 1987).

6 Several Morton-Thiokol engineers were troubled by the seals' poor performance. Long before the *Challenger* disaster Boisjoly wrote in a memo that the result of neglecting the problem "would be a catastrophe of the highest order—loss of human life." By August 1985 a seal task force had been established, but Bob Ebeling sent out this distress message: "HELP! The seal task force is constantly being delayed by every possible means. . . . This is a red flag." What else could or should these engineers have done in the months before *Challenger's* last flight?

7 On October 4, 1930, the British airship *R 101* crashed about 8 hours into its maiden voyage to India. Of the fifty-four persons aboard, only six survived. Throughout the craft's design and construction, Air Ministry officials and their engineers had been driven by political and competitive forces described by Shute (1954), Higham (1961), Robinson (1973), Meyer (1981), and Squires (1986). Shute, who had worked on the rival, commercial *R 100* wrote in his memoir, *Slide Rule*, that "if just one of [the men at the Air Ministry] had stood up [at a conference with Lord Thomson] and had said, 'This thing won't work, and I'll be no party to it. I'm sorry, gentlemen, but if you do this, I'm resigning' . . . the disaster would almost certainly have been averted. It was not said, because the men in question put their jobs before their duty" (Shute, 1954, 140). Examine the *R 101* case and compare it with the *Challenger* case.

CODES OF ETHICS

Invoking a code of ethics for engineers might have helped Dan Applegate and Roger Boisjoly with impressing their safety concerns on management. Such a use is one of the most important roles of a code. We shall examine it along with other prominent functions, prominent in terms of both positive and negative consequences. It is suggested that in reading this section the reader examine the sample codes of ethics given in the Appendix as if they were checklists for experimenters.

Roles of Codes

Inspiration and Guidance Codes provide a positive stimulus for ethical conduct and helpful guidance and advice concerning the main obligations of engineers. Often they succeed in inspiring by using language with positive overtones. This can introduce a large element of vagueness, as in phrases like "safeguard the public safety, health, and welfare," a vagueness which may lessen their ability to give concrete guidance. Sometimes lofty ideals and exhortative phrases are gathered into separate documents, such as *Faith of the Engineer*, published by the Accreditation Board for Engineering and Technology (ABET), which succeeded the Engineering Council for Professional Development (ECPD). *Faith of the Engineer* is reprinted in the Appendix along with several other codes or fundamental canons of ethics.

Since codes should be brief to be effective, they offer mostly general guid-

ance. More specific directions may be given in supplementary statements or guidelines. These tell how to apply the code. Further specificity may also be attained by the interpretation of codes. This is done for engineers by the National Society of Professional Engineers. It has established a Board of Ethical Review which applies the Society's code to specific cases and publishes the results in *Professional Engineer* and in periodic volumes entitled *NSPE Opinions of the Board of Ethical Review.*

For inclusion in the Appendix we have selected the codes of the following societies: the Accreditation Board for Engineering and Technology (ABET), the American Association of Engineering Societies (AAES), the National Society of Professional Engineers (NSPE), and the Institute of Electrical and Electronics Engineers (IEEE). The ABET code is accompanied by a set of guidelines which can appear separately or intermeshed with the fundamental canons. The latter format is sometimes followed by the American Society of Civil Engineers (ASCE), which has adopted the code and guidelines of ABET. Among other societies which subscribe to the ABET code and guidelines is the American Society of Mechanical Engineers (ASME).

A number of companies (for example, Bechtel, Hughes Aircraft, McDonnell-Douglas) have instituted their own codes. These tend to concentrate on the moral issues encountered in dealing with vendors and clients, particularly the U.S. federal government.

Support Codes give positive support to those seeking to act ethically. A publicly proclaimed code allows an engineer who is under pressure to act unethically to say: "I am bound by the code of ethics of my profession, which states that...." This by itself gives engineers some group backing in taking stands on moral issues. Moreover, codes can potentially serve as legal support in courts of law for engineers seeking to meet work-related moral obligations.

Deterrence and Discipline Codes can serve as the formal basis for investigating unethical conduct. Where such investigation is possible, a prudential motive for not acting immorally is provided as a deterrent. Such an investigation generally requires paralegal proceedings designed to get at the truth about a given charge without violating the personal rights of those being investigated. In the past, engineering professional societies have been reluctant to undertake such proceedings because they have lacked the appropriate sanctions needed for punishment of misconduct. Unlike the American Bar Association and some other professional groups, engineering societies cannot revoke the right to practice engineering in this country. Yet the American Society of Civil Engineers, for example, does currently suspend or expel members whose professional conduct has been proven unethical, and this alone can be a powerful sanction when combined with the loss of respect from colleagues and the local community that such action is bound to produce.

Education and Mutual Understanding Codes can be used in the classroom and elsewhere to prompt discussion and reflection on moral issues and

to encourage a shared understanding among professionals, the public, and government organizations concerning the moral responsibilities of engineers. They can help do this because they are widely circulated and officially approved by professional societies.

Contributing to the Profession's Public Image Codes can present a positive image to the public of an ethically committed profession. Where the image is warranted, it can help engineers more effectively serve the public. It can also win greater powers of self-regulation for the profession itself, while lessening the demand for more government regulation. Where unwarranted, it reduces to a kind of window dressing that ultimately increases public cynicism about the profession.

Protecting the Status Quo Codes establish ethical conventions, which can help promote an agreed upon minimum level of ethical conduct. But it can also stifle dissent within the profession. On occasion this has positively discouraged moral conduct and caused serious harm to those seeking to serve the public. In 1932, for example, two engineers were expelled from the American Society of Civil Engineers for violating a section of its code forbidding public remarks critical of other engineers. Yet the actions of those engineers were essential in uncovering a major bribery scandal related to the construction of a dam for Los Angeles County (Layton, 1980, 17).

Promoting Business Interests Codes can place "restraints of commerce" on business dealings with primary benefit to those within the profession. Basically self-serving items in codes can take on great undue influence. Obviously there is disagreement about which, if any, entries function in these ways. Some engineers believe that in the past the codes were justified in forbidding competitive bidding, while others agree with the decision of the Supreme Court in the case of the National Society of Professional Engineers vs. the United States (April 25, 1978) that such a restriction is inappropriate.

Codes and the Experimental Nature of Engineering

Given that codes may play all these roles, which functions are the most valuable and therefore should be emphasized and encouraged? This is an important question, if only because its answer can greatly influence the very wording of codes. For example, if the disciplinary function is to be emphasized, every effort would have to be made to ensure clear-cut and enforceable rules. This would also tend to make statements of minimal duty predominant, as with standards and laws, rather than statements concerned with higher ideals. By contrast, if the emphasis is to be on inspiration, then statements of high ideals might predominate. Nothing is less inspirational than arid, legalistic wordings, and nothing is less precise than highly emotional exhortations.

The perspective of engineering as social experimentation provides some help in deciding which functions should be primary in engineering codes. It

clearly emphasizes those which best enable concerned engineers to express their views freely—especially about safety—to those affected by engineering projects. Only thus can clients and the public be educated adequately enough to make informed decisions about such projects. But as we have already noted and will discuss in more detail later, contemporary working conditions within large corporations do not always encourage this freedom of speech—conditions for which a code of ethics can provide an important counterbalance. Thus the supportive function seems to us of primary importance.

The guidance, inspirational, and educational functions of engineering codes are important also, as is their role in promoting mutual understanding among those affected by them. In seeking to create a common understanding, however, code writers must take every precaution to allow room for reasonable differences between individuals. Wordings in past codes, for example, sometimes used religious language not acceptable to many who did not share that orientation. Codes, we must bear in mind, seek to capture the essential substance of professional ethics; they can hardly be expected to express the full moral perspective of every individual.

The disciplinary function of engineering codes is in our view of secondary importance. There are scoundrels in engineering, as there are everywhere. But when exposed as such, they generally fall subject to the law. Developing elaborate paralegal procedures within professional societies runs the risk of needlessly and at considerable cost duplicating a function better left to the real legal system. At most, enforcement of professional ethics by professional societies should center upon areas that are not covered by law and that can be made explicit and clear-cut, preferably in separate code sections specifically devoted to those areas. In any case, the vast majority of engineers can be counted on to act responsibly in moral situations unless *discouraged* from doing so by outright threats and lack of support on the part of employers.

Probably the worst abuse of engineering codes in the past has been to restrict honest moral effort on the part of individual engineers in the name of preserving the profession's public image and protecting the status quo. Preoccupation with keeping a shiny public image may silence the healthy dialogue and lively criticism needed to ensure the public's right to an open expression. And an excessive interest in protecting the status quo may lead to a distrust of the engineering profession on the part of both government and the public. The best way to *increase* trust is by encouraging and aiding engineers to speak freely and responsibly about the public safety and good as they see it. And this includes a tolerance for criticisms of the codes themselves. Perhaps the worst thing that can happen is for codes to become "sacred documents" that have to be accepted uncritically.

Limitations of Codes

Most codes are limited in several major ways. Those limitations restrict codes to providing only very general guidance, which in turn makes it essential for engineers to exercise a personal moral responsibility in their role as social ex-

perimenters rather than to expect codes to solve their moral problems by serving as simple algorithms. The limitations of codes are as follows.

First, as we have already mentioned, codes are restricted to general and vague wording. Because of this they are not straightforwardly applicable to all situations. After all, it is not humanly possible to foresee the full range of moral problems that can arise in a complex profession like engineering. New technical developments and shifting social and organizational structures combine to generate continually new and often unpredictable conditions. And even in the case of foreseeable situations it is not possible to word a code so that it will apply in every instance. Attempting to do so would yield something comparable to the intricate set of laws governing engineering rather than a manageable code.

A sense of responsibility is indispensable for the skillful and at times creative application of code guidelines to concrete situations. It is also the only way certain abuses of codes can be avoided—for example, abuses such as special interpretations being placed on general entries, or legalistic glosses on specific entries, to serve the private gain or convenience of specific individuals or groups.

Second, it is easy for different entries in codes to come into conflict with each other. Usually codes provide no guidance as to which entry should have priority in those cases, thereby creating moral dilemmas.

For example, take the following two former entries from the National Society of Professional Engineers (NSPE) code. Section 1: "The Engineer will be guided in all his professional relations by the highest standards of integrity, and will act in professional matters for each client or employer as a faithful agent or trustee." Section 2: "The Engineer will have proper regard for the safety, health, and welfare of the public in the performance of his professional duties." Which was the more applicable in the DC-10 case mentioned in Chap. 2, where an engineer was told to ignore a situation he believed threatening to the public safety on the basis of a business decision made in the interests of his company?

Recent codes have attempted to address this important area of potential conflict. The NSPE code now states: "Engineers shall hold paramount the safety, health, and welfare of the public in the performance of their professional duties." The word "paramount" means "most important or superior in rank." But even so it is unclear that the provision means engineers should never, under any circumstances, follow a client's or company's directives because they believe those directives might not serve the best interests of the public. This is an issue we will return to in Part III of our book. But here we emphasize again the need for responsible engineers who are able to make reasonable assessments of what "paramount" amounts to in cases where two professional obligations conflict.

A third limitation on codes is that they cannot serve as the final moral authority for professional conduct (Ladd, 1980, 154). To accept the current code of a professional society as the last moral word, however officially endorsed

it may be, would be to lapse into a type of Ethical Conventionalism. It will be recalled that Ethical Conventionalism is the view that a particular set of conventions, customs, or laws is self-certifying and not to be questioned simply because it is the set in force at a given time or for a given place. Such a view, of course, rules out the possibility of criticizing that set of conventions from a wider moral framework.

Consider once again the following entry in the pre-1979 versions of the NSPE code: "He [the engineer] shall not solicit or submit engineering proposals on the basis of competitive bidding." This prohibition was felt by the NSPE to best protect the public safety by discouraging cheap engineering proposals which might slight safety costs in order to win a contract. Critics of the prohibition, however, contended that it mostly served the self-interest of engineering firms and actually hurt the public by "preventing" the lower prices that might result from greater competition. In a 1978 decision, National Society of Professional Engineers vs. United States, the Supreme Court ruled that the ban on competitive bidding was unconstitutional and not appropriate in a code of ethics.

The point here is not who holds the correct moral view on this issue—that is a matter of ongoing debate and discussion. And indeed, it is precisely our point that no pronouncement by a code current at any given time should ever be taken as the final word silencing such healthy debates. Codes, after all, represent a compromise between differing judgments, sometimes developed amidst heated committee disagreements. As such, they have a great "signpost" value in suggesting paths through what can be a bewildering terrain of moral decision maker. But equally as such they should never be treated as "sacred canon."

The fourth limitation of codes results from their proliferation. Andrew Oldenquist (a philosopher) and Edward Slowter (an engineer and former NSPE president) point out how the existence of separate codes for different professional engineering societies can give members the feeling that ethical conduct is more "relative" than it is, and how it can convey to the public the view that none of the codes is "really right." But Oldenquist and Slowter have also demonstrated the substantial agreement to be found among the various engineering codes. These authors summarize the core concepts in each and arrange them in order of significance as having to do with (1) the public interest, (2) qualities of truth, honesty, and fairness, and (3) professional performance. They emphasize in their 1979 paper that the time has come for adoption of a unified code (Oldenquist and Slowter, 1979, 8–11). The ABET and AAES codes (see Appendix) are by no means perfect (see Study Question 4), but they are steps in the right direction.

Study Questions

1 Apply a code of ethics taken from the Appendix—or from the collection of Canadian engineering codes cited by Morrison and Hughes (1988) —to the short

cases presented as study questions on page 14. Discuss the possible effectiveness of the code(s) as a deterrent to unethical behavior in these cases.

2 Comment on the following passage: "A code only sets the limits beyond which behavior will be condemned, and the moral level is not high when all or most of those who live under it always act within a hairline of those limits. Codes, in fact, are for criminals and competitors, not for professions that want to be known as dedicated" (Barzun, 1978, 67). Specifically, is this true of the engineering codes given in the Appendix?

3 Respond to the following claim: "Even if substantial agreement could be reached on ethical principles and they could be set out in a code, the attempt to impose such principles on others in the guise of ethics contradicts the notion of ethics itself, which presumes that persons are autonomous moral agents" (Ladd, 1980, 154). Is the idea of an officially prescribed, authoritative code of ethics somehow incompatible with an appreciation of the importance of moral autonomy in individuals?

4 Critique the following codes given in the Appendix:

a The AAES Code. Examples of issues for discussion are given by Unger (1986): (*i*) The fundamental principle demands "...concern for the public health and safety." Should "welfare" have been included? (*ii*) Canon 1 restricts activity to "areas of competence and experience." How does an engineer gain experience or deal with new technology? What would be the role of the generalist or manager? (*iii*) Canon 5 might conflict with Canon 6. Which is more binding? (*iv*) Canon 7 omits professional growth of subordinates. Is it important?

b The NSPE code. Consider the following two entries in the 1981 Code of the National Society of Professional Engineers. (*i*) "Engineers shall cooperate in extending the effectiveness of the profession by interchanging information and experience with other engineers and students." (*ii*) "Engineers shall not disclose confidential information concerning the business affairs or technical processes of any present or former client or employer without his consent." Suppose that the two entries come into conflict—for instance, when improving the knowledge and skill of another engineer or student might best be done by passing on confidential information. Which entry should take precedence, and why? Do you think the code should be modified so as to explicitly state which entry should take precedence?

c Other codes. Closely examine the other codes in the Appendix. Are there any entries in them which you think should not be there? Why? Are there any important omissions in the codes?

5 Discuss the Pennwalt advertisement, Fig. 3-2, in light of your understanding of engineering codes of ethics.

A BALANCED OUTLOOK ON LAW

The 1969 Santa Barbara offshore spill of 235,000 gallons of crude oil blackened 30 miles of spectacular beaches, damaged wildlife, and hurt the local tourist trade. Predictably, the disaster prompted demands for new laws and tighter controls to prevent such occurrences in the future (Lawless, 1977, 233–247). A group of Southern Californians staged a burning of gasoline credit cards issued by the offending oil company, Union Oil, only to be taken to task by a local newspaper for taking the wrong aim. The newspaper ar-

A code of ethics isn't something you post on the bulletin board.

It's something you live every day.

Suddenly everybody seems to be rediscovering ethics.

In the business community, in Congress, on the campus and in the pulpit.

We think the trend is healthy. And needed. So we'd like to disclose a discovery of our own on this subject.

We found a long time ago that when it comes to any sort of corporate decree, the more you reduce it to writing the more you reduce participation.

It's much better, we learned, to create a working environment in which communication is a two-way process. And corporate goals are shared.

So that your code of ethics is expressed not in a news release, but in the release of appropriate thought and action.

Nobody's perfect, but it seems to work.

As our chairman put it: "The character of this company is simply a reflection of how Pennwalt people think and act. *That's* our code of ethics."

And so it is.

Admittedly, it's an approach that places more stress on the integrity and good judgment of our people than on manuals from Personnel. (A *lot* more stress.)

But it pays off. In pride. In performance. In a belief that the work we do is important. And in the enhancement of our worldwide reputation.

You might say it's the difference between a bulletin that goes up on the board, and the life that goes on every day.

(We have a brief booklet on corporate citizenship which we believe covers this subject. If you'd like one, just write our Director of Corporate Communications.)

Pennwalt Corporation, Three Parkway, Philadelphia, Pa. 19102.

For 126 years we've been making things people need—including profits.

PENNWALT
CHEMICALS ■ EQUIPMENT
HEALTH PRODUCTS

Courtesy of Penwalt Corporation.

FIGURE 3-2
A statement on codes of ethics (see Study Question 5).

gued that the gas station operators, who would suffer the most from a boycott, were not at fault. The real offenders were the federal authorities who required less stringent safeguards in offshore drilling than did California state authorities, it was claimed.

Yet we might well ask, who would be involved in drafting safety regulations for offshore drilling? Obviously experienced petroleum engineers, geologists, and well drillers, members of the same group which had prepared the state regulations and who—in their capacity as oil company employees—had also conducted the drilling off the coast of Santa Barbara. If expert knowledge was available, then why was it not applied, law or no law?

It is worth noting that some safeguards were indeed required by federal law. Following the Santa Barbara incident, then Secretary of the Interior Walter Hickel ordered an inspection of the thousands of offshore oil wells, mostly in the Gulf of Mexico. The inspection showed that hundreds lacked mandatory safety chokes. Hickel ordered prosecutions and later justified his tough approach to pollution with what has been called "Hickel's law": "You've got to hit them [i.e., polluters] with a two-by-four to make them believe you" (Rosenbaum, 1977, 129).

Is it really necessary to burden engineering practice with ever more—and increasingly restrictive—rules? Earlier we discussed the bases for responsible action. Here we shall examine the role of formal rules and their ethical implications. The model of engineering as social experimentation will assist us again as we consider the interaction of rules with the engineering process. The problem of product liability and safe design will be postponed until we take up a more detailed analysis of risk in Chap. 4.

A Regulated Society

In order to live, work, and play together in harmony as a society, we need to carefully balance individual needs and desires against collective needs and desires. Ethical conduct, which by definition includes a strong element of altruism, provides such a balance. Unfortunately people all too frequently disagree on what constitutes right action in specific instances, even when they agree on ultimate goals. At such times we need to negotiate, and if a compromise can be agreed upon, it should be recorded for repeated reference and use.

Engineers can play an active role in establishing or changing rules as well as in enforcing them. Indeed, some people would say that the engineer's ethical duties should be limited to just such activities—in addition to following accepted rules of conduct, of course (Florman, 1978, 30–33).

At various times in history, and in various countries, engineers have had less say in how rules affecting their work were made or carried out, except perhaps for a few who were among a ruler's trusted advisors; often engineers were merely subject to those rules. We assume that the time of Hammurabi fits this description.

1758 B.C.: Babylon's Building Code Hammurabi as King of Babylon was concerned with strict order in his realm, and he decided that the builders of his time should also be governed by his laws. Thus he decided as follows:

> If a builder has built a house for a man and has not made his work sound, and the house which he has built has fallen down and so caused the death of the householder, that builder shall be put to death. If it causes the death of the householder's son, they shall put that builder's son to death. If it causes the death of the householder's slave, he shall give slave for slave to the householder. If it destroys property he shall replace anything it has destroyed; and because he has not made sound the house which he has built and it has fallen down, he shall rebuild the house which has fallen down from his own property. If a builder has built a house for a man and does not make his work perfect and the wall bulges, that builder shall put that wall into sound condition at his own cost (Hammurabi; also quoted by Firmage, 1980, 7).

The substantive or normative part of Babylon's building code is admirably succinct. The procedural aspects would find little approval today, although we cannot help but wistfully reflect on how small a bureaucracy it probably took to maintain standards. One can imagine how builders passed on their carefully drawn rules for sound design from generation to generation. There was indeed a powerful incentive for self-regulation! In other words, the law was broad and the specifics of how to comply with it were left to those presumably best able to formulate them for each application—the builders themselves. We might note that this was by no means a simple matter, for "the Babylonians found only deep alluvium in their flood plains between the Tigris and the Euphrates, which settled under the weight of their cities" (Sowers, 1970, 389).

Let us turn to another example, some four millennia later. In this case, procedural aspects and regulations in detail took the form of ready-made standards.

A.D. 1852: The U.S. Steamboat Code Early steam engines were large and cumbersome. So to make them more practical for use, James Watt, and later Oliver Evans and Richard Trevethick, increased steam pressure, did away with the condenser in some models, and thus ushered in the age of compact, portable sources of motive power. In spite of these pioneers' careful calculations and guidelines, however, boiler explosions were frequent, particularly on steamboats. Nowhere was the problem as acute as in the United States, where riverboats were vying for trade on the great midwestern rivers. Races were common, boilers were stressed beyond their limits, and safety valves were disabled to keep steam pressure up; 233 explosions contributed to a total of 2563 persons killed and 2097 injured during the period 1816 to 1848. One explosion alone, on the *Moselle* in Cincinnati in 1838, claimed 151 lives (Burke).

Demands for safety rules finally moved Congress to exert its river and interstate regulatory powers. Steamboat interests objected. It was argued that

the prudent self-interest of steamboat owners and operators would in itself dictate caution. Cumbersome rules and an unyielding bureaucracy were predicted. But self-regulatory commitments by owners and operators were clearly not in evidence. So in 1838 a law was passed which provided for the inspection of the safety features of ships and their boilers and engines. The occurrence of an explosion was to be taken as prima facie evidence of negligence and any loss of life was to be considered manslaughter.

But the 1838 law turned out to be ineffective. Shipowners could find corruptible inspectors. Even honest inspectors were not much help. They had no training and the law did not specify how a safety check should be conducted. Nevertheless, after a safety check was carried out, a shipowner could claim to be blameless. Boiler explosions continued unabated.

Among those who were troubled by the situation was Alfred Guthrie, an engineer from Illinois. Guthrie had inspected, at his own expense, about 200 steamboats to learn the causes of boiler explosions and written a report on his findings. His recommendations were published by a Senator Shields of Illinois and included in Senate documents. By 1852, when a new steamboat bill came before Congress, the groundwork had been carefully laid, and an effective law was passed. Guthrie was made the first supervisor of the regulatory agency established by the law.

Congress was able to intervene as it did because of its powers to regulate interstate shipping. But even then it was left to ad hoc associations, insurance companies, and later the American Society of Mechanical Engineers to promulgate the standards which would govern the manufacture of steam boilers and their operation in mines, factories, and railroads. In France, boiler safety standards were earlier and more rapidly promulgated under the more centralized state authority of the Napoleonic code. Between 1823 and 1830 a committee of engineers, assisted by prominent scientists of the time, developed accurate steam tables, stress values for metals, and design standards which called for hemispherical end plates and initial testing of boilers at three times their expected operating pressure. France had very few boiler explosions thereafter—nor did the United States after 1852.

The Trend Toward Greater Detail

In Hammurabi's time one could let the law take care of building failures *after* the structure had failed. While many houses may have crumbled, there were probably not many casualties associated with any one occasion (unless an earthquake had struck). However, when 150 passengers and crew members can be killed all at once by a boiler explosion and the ship is likely to sink, there will be demands for rules which prevent such accidents from happening in the first place. As technology's machines became more complex, simplicity in rule-making appeared to be doomed. The 1852 steamboat law even had to regulate the qualifications of steamboat inspectors.

But lawmakers cannot be expected always to keep up with technological development. Nor would we necessarily want to see laws changed with each

new innovation. What is needed are regulating agencies and commissions—the Food and Drug Administration (FDA), Federal Aviation Agency (FAA), and the Environmental Protection Agency (EPA) are examples of these in the United States—to fill the void. These agencies employ experts who can set up precise regulations. And even though they are independent and belong to neither the judicial nor the executive branches of government, their rules have, for all practical purposes, the effect of law.

Industry tends to complain that excessive restrictions are imposed on it by regulatory agencies. But one needs to reflect on why regulations may have been necessary in the first place. Take, for example, the U.S. Consumer Product Safety Commission's rule for baby cribs which specifies that "the distance between components (such as slats, spindles, crib rods, and corner posts) shall not be greater than 2⅜ inches at any point." This rule came about because some manufacturers of baby furniture had neglected to consider the danger of babies strangling in cribs or had neglected to measure the size of babies' heads (Lowrance, 1976, 134).

Again, why must regulations be so specific when broad statements would appear to make more sense? When the EPA adopted rules for asbestos emissions in 1971, it was recognized that strict numerical standards would be impossible to promulgate. Asbestos dispersal and intake, for example, are difficult to measure. So, being reasonable, EPA specified a set of work practices to keep emissions to a minimum—that asbestos should be wetted down before handling, for example, and disposed of carefully.

> [A wrecking company], after promising repeatedly to comply with the rules, came along and demolished buildings without taking any of the precautions—thereby endangering its workers and the surrounding community. The violations were so blatant, EPA felt, and civil procedures so inadequate under the Clean Air Act, that the agency asked for and received a criminal indictment.... The U.S. Supreme Court overruled the Court of Appeals... and threw out the charges. Thanks to the High Court's technical illiteracy, EPA might now be justified in attempting to prescribe voluminous measurement techniques covering all possible asbestos-generating situations since its reasonableness led to an all but unenforceable rule. The engineering community would then snicker and joke about EPA's foolishness. Wouldn't it be better for the construction industry to police itself, and for demolition instructions with regard to asbestos to be clearly specified by contract? (S. Ross, 1978, 6) [Modifications in the Clean Air Act eventually permitted EPA to issue enforceable rules on work practices, and now the Occupational Safety and Health Administration is also involved.]

Industrial Standards

There is one area in which industry usually welcomes greater specificity, and that is in regard to standards. Standards facilitate the interchange of components, they serve as ready-made substitutes for lengthy design specifications, and they decrease production costs.

Standards consist of explicit specifications which, when followed with care, assure that stated criteria for interchangeability and quality will be attained.

Examples range from automobile tire sizes and load ratings to computer languages. Table 3-1 lists purposes of standards and gives some examples to illustrate those purposes.

Standards are established by companies for in-house use, are adopted by professional associations and trade associations for industrywide use, and may also be prescribed as parts of laws and official regulations. The latter would be examples of mandatory standards, which frequently arise from lack of adherence to voluntary standards.

Standards do not help the manufacturers only; they also benefit the client and the public. They preserve some competitiveness in industry by reducing overemphasis on name brands and giving the smaller manufacturer a chance to compete. They assure a measure of quality and thus facilitate more realistic trade-off decisions.

Standards can also be a hindrance at times. For many years they were mostly descriptive, specifying, for instance, how many joists of what size should support a given type of floor. Clearly such standards tended to stifle innovation. The move to performance standards, which in the case of a floor may merely specify the required load-bearing capacity, has alleviated that problem somewhat. But other difficulties can arise when special interests (e.g., manufacturers, trade unions, exporters and importers) manage to impose unnecessary provisions on standards, or remove important provisions from them, to secure their own narrow self-interest. Requiring metal conduits for home wiring is one example of this problem. Modern conductor coverings have eliminated the need for metal conduit in numerous applications, but many localities still require it. Its use sells more conduit and labor time for installation.

There are standards nowadays for practically everything, it seems, and

TABLE 3-1
TYPES OF STANDARDS

Criterion	Purpose	Selected examples
Uniformity of physical properties and functions	Accuracy in measurement; interchangeability; ease of handling	Standards of weights; screw thread dimensions; standard time; film size
Safety and reliability	Prevention of injury, death, and loss of income or property	National Electric Code; boiler code; methods of handling toxic wastes
Quality of product	Fair value for price	Plywood grades; lamp life
Quality of personnel and service	Competence in carrying out tasks	Accreditation of schools; professional licenses
Use of accepted procedures	Sound design; ease of communications	Drawing symbols; test procedures
Separability	Freedom from interference	Highway lane markings; radio frequency bands

consequently we frequently assume that stricter regulation exists than may actually be the case. The public tends to trust implicitly the National Electrical Code in all matters related to power distribution and wiring, but how many people realize that this code, issued by the National Fire Protection Association, is primarily oriented toward *fire* hazards? Only recently have its provisions against electric shock begun to be strengthened. Few consumers know that an Underwriter Laboratories seal prominently affixed to the cord of an electrical appliance may pertain to the cord only and not to the rest of the device. In a similar vein, a patent notation inscribed on the handle of a product may refer just to the handle, and then possibly only to the design of the handle's appearance.

Sometimes standards are thought to apply when in actuality there is no standard at all. An example can be found in the widely varying worth and quality of academic degrees—doctorates are even available from mail order houses. Appearances can be misleading in this respect. Years ago when competing foreign firms were attempting to corner the South American market for electrical fixtures and appliances, one manufacturing company had a shrewd idea. It equipped its light bulbs with extra-long bases and threads. These would fit into the competitors' lamp sockets and its own deep sockets. But the competitors' bulbs would not fit into the deeper sockets of its own fixtures (see sketch in Fig. 3-3). Yet so far as the unsuspecting consumer was concerned, all the light bulbs and sockets continued to look alike.

Problems with the Law in Engineering

The legal regulations which apply to engineering and other professions are becoming more numerous and more specific all the time. We hear many complaints about this trend, and a major effort to "deregulate" various spheres of our lives is currently underway. Nevertheless, we continue to hear cries of "there ought to be a law" whenever a crisis occurs or a special interest is threatened.

FIGURE 3-3
The light bulb story. (*a*) Long base, deep socket: firm contact. (*b*) Short base, deep socket: no contact. (*c*) Long base, shallow socket: firm contact.

This is not surprising. We pride ourselves on being a nation that lives under the rule of law. We even delegate many of our decisions on ethical issues to an interpretation of laws. And yet this emphasis on law can cause problems in regard to ethical conduct quite aside from the more practical issues usually cited by those who favor deregulation.

For example, one of the greatest moral problems in engineering, and one fostered by the very existence of minutely detailed rules, is that of *minimal compliance*. Companies or individuals hunt around for loopholes in the law that will allow them to keep to its letter while violating its spirit. Or hard-pressed engineers sometimes find it convenient to refer to standards with specifications already prepared as a substitute for original thought, perpetuating the "handbook mentality" and the repetition of mistakes.

Minimal compliance led to the tragedy of the *Titanic* (Wade, 1980, 68): Why should that ship have been equipped with enough lifeboats to accommodate all its passengers and crew when British regulations in effect at the time did not require it? Or why should the Tampa Bay Bridge have been designed with possible ship collisions in mind when the code required that only wind loads, not impact loads, be considered in the calculation of horizontal forces?

On the other hand, remedying the situation by continually updating laws or regulations with further specifications may also be counterproductive. Not only will the law inevitably lag behind changes in technology, leading to a judicial vacuum; there is also the danger of overburdening the rules and the regulators. As Robert Kates puts it:

> If cooperation is not forthcoming—if the manufacturer, for example, falsifies or fails to conduct safety tests—there is something akin to the law of infinite regress in which the regulator must intrude more and more expensively into the data collection and evaluation process. In the end, the magnitude of the task overwhelms the regulators (Kates, 1977, 32).

The public is frequently lulled into a sense of security by the passage of new laws. Yet many laws are "nonlaws"—that is, laws without enforceable sanctions. These merely serve as window dressing—a false display of caring. Or a law may be burdened intentionally by its opponents with so many unreasonable provisions that a repeal will not be far off. Thus there is a need for the critical examination of many laws—and of their sources. Even Adam Smith was moved to make the following observation:

> The proposal of any new law or regulation of commerce which comes from the capitalist class ought always to be listened to with great skepticism, and ought never to be adopted until it has been examined, not only with the most scrupulous, but with the most suspicious attention (Jenkins, 1948, 156).

And still another problem with and occasion for frustration with the law is the apparent immunity with which powerful interests, including the government, can violate laws when they think they can get away with

it by inviting would-be challengers to face them in lengthy and costly court proceedings.

The Proper Role of Laws in Engineering

Society's attempts at regulation have indeed often failed, and in various ways. But it would be wrong to write off rule making and rule following as futile. Good laws, effectively enforced, clearly produce benefits. They authoritatively establish reasonable minimal standards of professional conduct and provide at least a self-interested motive for most people and corporations to comply with those standards. Moreover, they serve as a powerful support and defense for those who wish to act ethically in situations where ethical conduct might be less than welcome. By being able to point to a law, one can feel freer to act as a responsible engineer.

We contend that to view engineering as social experimentation can provide engineers with a proper perspective on laws and regulations. And the rules which govern engineering practice should not be devised or construed as rules of a game but as rules of responsible experimentation.

Such a view places great responsibility on the engineer, who is intimately connected will his or her "experiment" and responsible for its safe conduct; moreover, it suggests the following conclusions: Precise rules and enforceable sanctions are appropriate in cases of ethical misconduct which involve violations of well-established and regularly reexamined procedures that have as their purpose the safety and well-being of the public. Little of an experimental nature is probably occurring in such standard activities, and the type of professional conduct required is most likely very clear-cut. In areas where experimentation is involved more substantially, however, rules must not attempt to cover all possible outcomes of an experiment, nor must they force the engineer to adopt a rigidly specified course of action. It is here that regulations should be broad, but so written as to hold the engineer accountable for his or her decisions.

Consider genetic "engineering," for example. One can foresee the time when genetic manipulation will be carried out in a routine manner under strict sets of guidelines. At present, however, the field is still so new that any rules will invariably leave uncovered some very important safety aspects. Rather than provide unintentional loopholes through such omissions, or convey a false sense of security to laboratory personnel, it would be better to issue only very general guidelines. The gist of these guidelines would be to place responsibility and accountability for unforeseen consequences on the experimenter.

Study Questions

1 How do the roles of standards, regulations, and laws differ with respect to engineering products and practice?

2 A growth in regulatory practices in the United States during the 1970s was followed by a reversal during the 1980s. Where should regulations go from here? Discuss the relevant factors from the standpoint of the engineer, the lawyer, and the (government) regulator. Discuss their roles in rule making. Consider the influences of rapidly changing technology. You may discuss these issues in generic terms or pick a particular industry and its regulator as an example (e.g., air transport and FAA; chemicals and EPA; electronic media and FCC; consumer products and FTC).

3 In 1975, Hydrolevel Corporation brought suit against the American Society of Mechanical Engineers (ASME), charging that two ASME volunteers, acting as agents of ASME, had conspired to interpret a section of ASME's Boiler and Pressure Vessel Code in such a manner that Hydrolevel's low-water fuel-cutoff for boilers could not compete with the devices built by the employers of the two volunteers. On May 17, 1982, the Supreme Court upheld the lower courts which had found ASME guilty of violating antitrust provisions and had opened the way for awarding of treble damages. (A U.S. District Court's award of $7.5 million had been found excessive by the Court of Appeals.) Writing on behalf of the 6 to 3 majority, Justice Harry A. Blackmun said: "When ASME's agents act in its name, they are able to affect the lives of large numbers of people and the competitive fortunes of businesses throughout the country. By holding ASME liable under the antitrust laws for the antitrust violations of its agents committed with apparent authority, we recognize the important role of ASME and its agents in the economy, and we help to ensure that standard-setting organizations will act with care when they permit their agents to speak for them." Acquaint yourself with the particulars of this case and discuss it as an illustration of the possible misuses of standards.

4 On February 26, 1972, the Buffalo Creek dam near Lorado, West Virginia, collapsed, "unleashing a wall of water that killed 118 persons and swept away four communities." A U.S. Senate labor subcommittee investigating the damage found that "lack of adequate design and construction measures as well as the poor planning and operation make all similar dams presently in use a serious hazard. . . . The safety factor slipped between the cracks of responsibility." Regulations of the U.S. Bureau of Mines called for inspections which had not been carried out. But, stated the Bureau's director, "Even if a bureau coalmine inspector had been at the dam site as the waters rose, his authority would have been limited to the issuance of an imminent danger order, withdrawing the mine workers on the mine property." It would not, he said, have "prevented the retaining dam from failing nor would it have been applicable to persons off the mine property in the path of the flood." The West Virginia Public Service Commission denied responsibility because it certifies dams for safety only at the time that a builder applies for a permit to build a dam. The Commission claims to have no jurisdiction over dams once they have been built (based on an Associated Press report in the *Los Angeles Times*, 1 June 1972).

A Governor's Ad Hoc Committee found that the dam had been built by a non-engineer, that inspectors should have been aware of problems, and that the engineering profession should have sounded a warning since some of its members were aware of the substandard construction. The registration system had failed in this instance, because "the specialty required by any engineer designing and constructing such a dam as that which failed, is not covered in any of the categories mentioned by the West Virginia State Registration Board. Moreover, since the technology of building such dams as this had not been developed, there was no way of

judging any competence in the persons constructing such dams" (from *The West Virginia Engineer*, December 1972, courtesy of Robert D. Miles, Purdue University).

Write an essay on the Buffalo Creek flood in which you touch upon the issues we have covered so far in this book. More technical information can be found in the book on dam failures by R. B. Jansen.

5 Should owners of passenger cars be protected against extensive front-end damage to their cars when they or other authorized drivers back-end trucks or high-riding off-road vehicles which have incompatible (or no) bumpers? Are there standards governing bumper location? What do they say, and are they enforced?

SUMMARY

Engineering is an inherently risky activity, usually conducted with only a partial knowledge of the underlying scientific laws about nature and society and often producing uncertain results and side effects. It lends itself to being viewed as an experiment on a societal scale involving human subjects. While it differs from standard experiments using control groups, it nevertheless imposes the same moral requirements on engineers that are imposed on researchers in other experimental areas involving human subjects. Most important, it requires the following: imaginative forecasting of possible bad side effects, and with this the development of an attitude of "defensive engineering"; careful monitoring of projects; respect for people's rights to give informed consent; and in general that engineers act as *responsible agents*.

Responsible agency, understood as a moral virtue, involves several features: (1) conscientious committment to live by moral values, (2) a disposition to maintain a comprehensive perspective on the context and possible consequences of one's actions, (3) autonomous, personal involvement in one's activities, and (4) an acceptance of accountability for the results of one's conduct.

There are many contemporary threats to efforts by engineers to act responsibly, as well as obstacles placed in the way of their respecting the public's right to have the knowledge needed for making informed decisions about engineering products and projects. Those threats and obstacles include the pressures caused by time schedules and organizational rules restricting free speech; the narrow division of labor which tends to cause moral "tunnel vision"; a preoccupation with legalities in a time of proliferating malpractice lawsuits; and the human tendency to divorce oneself from one's actions by placing all responsibility on an "authority" such as one's employer.

Codes of ethics promulgated by professional societies play a variety of roles: (1) inspiration, (2) guidance, (3) support for responsible conduct, (4) deterring and disciplining unethical professional conduct, (5) education and promotion of mutual understanding, (6) contributing to a positive public image of the profession, (7) protecting the status quo and suppressing dissent within the profession, and (8) promoting business interests through restraint of trade.

From the perspective of engineering as social experimentation, the emphasis of codes should be on support of responsible conduct, general guidance, and promotion of mutual understanding rather than on punishment; and the roles of protecting the status quo and promoting business should be avoided altogether. On the other hand, it should be kept in mind that codes are only a small part of engineering ethics. Their brevity renders them overly general and vague, so that some provisions occasionally contradict others. They also represent compromises between many differing viewpoints, the expression and discussion of which must never be stifled. Codes are anything but sacred writ, and should always be viewed as open to critical examination.

A balanced outlook on laws emphasizes both the necessity of laws and regulations and their limitations in governing engineering practice. Laws are necessary because people are not fully responsible and because the competitive nature of our free enterprise system does not always encourage the requisite moral initiative on the part of corporations. Their effects are limited because they encourage minimal compliance with their provisions and tend toward the kind of detailed regulation which can harm productivity and sometimes actually promote violations of the spirit of the law. Moreover, laws inevitably lag behind technological development.

The model of engineering as social experimentation allows for the importance of clear laws, effectively enforced. But it places equal emphasis on the moral responsibility of engineers—an emphasis that goes beyond merely following laws and is especially vital for those working at the frontiers of technological development.

CHAPTER 4

THE ENGINEER'S CONCERN FOR SAFETY

Pilot Dan Gellert was flying an Eastern Airlines Lockheed L-1011, cruising at an altitude of 10,000 feet, when he inadvertently dropped his flight plan. Being on autopilot control, he casually leaned down to pick it up. In doing so, he bumped the control stick. This should not have mattered, but immediately the plane went into a steep dive, scaring the 230 passengers no end. Badly shaken himself, Gellert was nevertheless able to grab the control stick and ease the plane back onto course. Though much altitude had been lost, the altimeter still read a stable 10,000 feet.

Not long before this incident, one of Gellert's colleagues had been in a flight trainer when the autopilot and the flight trainer disengaged, producing a crash on an automatic landing approach. Fortunately it all happened on simulation. But just a short time later, an Eastern Airlines L-1011 actually crashed on approach to Miami. On that flight there seemed to have been some problem with the landing gear, so the plane had been placed on autopilot at 2000 feet while the crew investigated the trouble. Four minutes later, after apparently losing altitude without warning while the crew was distracted, it crashed in the Everglades, killing 103 people.

A year later Gellert was again flying an L-1011 and the autopilot disengaged once more when it should not have done so. The plane was supposedly at 500 feet and on the proper glide slope to landing as it broke through a cloud cover. Suddenly realizing it was only at 200 feet and above a densely populated area, the crew had to engage the plane's full takeoff power to make the runway safely.

The L-1011 incidents point out how vulnerable our intricate machines and

control systems can be, how failures in their working can be caused by unanticipated circumstances, and how important it is to design for proper human-machine interactions whenever human safety is involved. The reader who is curious to find out what happened in the course of Gellert's frustrating efforts to seek corrective action is referred to his account, "Insisting on Safety in the Skies" (Westin, 1981, 17–30). Here we turn to a more general discussion of the role of safety as seen by the public and the engineer.

Members of the public are "active consumers" when they use appliances to mow the lawn, wash clothes, or toast bread. The same persons are "passive consumers" of gasoline, water, and electricity because they have less control over or power of selection with regard to the latter commodities or services. Finally, they are mere "bystanders" when they are exposed to pollution from sources beyond their control. The "engineers" are those members of the engineering and allied professions who are knowledgeable in the design, manufacture, application, and operation of a specific engineered product. They may act as individual entrepreneurs or employees who produce and sell engineered products, buy and operate them, or educate persons to perform those activities. Gellert fit the operator category of engineer, while his passengers were passive consumers.

Thus typically several groups of people are involved in safety matters, each with its own interests at stake. If we now consider that within each group there are differences of opinion regarding what is safe and what is not, it becomes obvious that "safety" can be an elusive term. It behooves us, therefore, to decide upon a working definition of safety. And to help us understand the subject even more fully, we will discuss it in conjunction with the term "risk." Following a look at these basic concepts, we will then turn to safety and risk assessment and methods of reducing risk (increasing safety). Finally, by way of examining the nuclear power plant accidents at Three Mile Island and Chernobyl, we will consider the implications of an ever-growing complexity in engineered systems and the ultimate need for "safe exits."

SAFETY AND RISK

We demand safe products and services because we do not wish to be threatened by potential harm, but we also realize that we may have to pay for this safety. To complicate matters, what may be safe enough for one person may not be so for someone else—either because of different perceptions about what is safe or because of different predispositions to harm. For example, a power saw in the hands of a child will never be as safe as it can be in the hands of an adult. And a sick adult is more prone to suffer ill effects from air pollution than is a healthy adult.

Absolute safety, in the sense of a degree of safety which satisfies all individuals or groups under all conditions, is neither attainable nor affordable.

Yet it is important for our discussion here that we come to some understanding of what we mean by safety.

The Concept of Safety

One approach to defining "safety" would be to render the notion thoroughly subjective by defining it in terms of whatever risks a person judges to be acceptable. Such a definition was given by William W. Lowrance: *"A thing is safe if its risks are judged to be acceptable"* (Lowrance, 1976, 8). This approach helps underscore the notion that judgments about safety are tacitly value judgments about what is acceptable in the way of risk to a given person or group. Differences in appraisals of safety are thus correctly seen as reflecting differences in values.

Lowrance's definition, however, needs to be modified, for it departs too far from our common understanding of safety. This can be shown if we consider three types of situations that can arise. Imagine, first, a case where we seriously *underestimate* the risks of something—say of using a toaster we see at a garage sale. On the basis of that mistaken view, we judge it to be very safe and buy it. On taking it home and trying to make toast with it, however, it sends us to the hospital with a severe electric shock and burn. Using the ordinary notion of safety, we conclude we were wrong in our earlier judgment: The toaster was not safe at all! Given our values and our needs, its risks should not have been judged acceptable earlier. Yet by Lowrance's definition we would be forced to say that prior to the accident the toaster was entirely safe since, after all, at that time we had judged the risks to be acceptable.

Consider, second, the case where we grossly *overestimate* the risks of something. For example, we irrationally think fluoride in drinking water will kill a third of the populace. According to Lowrance's definition, the fluoridated water is unsafe, since we judge its risks to be unacceptable. It would, moreover, be impossible for someone to reason with us to prove that the water is in reality safe. For again, according to his definition, the water became unsafe the moment we judged the risks of using it to be unacceptable for us. But of course, our ordinary concept of safety allows us to say the water has been perfectly safe all along, in spite of such irrational judgments.

Third, there is the situation in which a group makes no judgment at all about whether the risks of a thing are acceptable or not—they simply do not think about it. By Lowrance's definition this means the thing is neither safe nor unsafe with respect to that group. Yet this is somewhat paradoxical, given our ordinary ways of thinking about safety. For example, we normally say that some cars are safe and others unsafe, even though many people may never even think about the safety of the cars they drive.

The point is that there must be at least some objective point of reference outside ourselves which allows us to decide whether our judgments about safety are correct or not. An adequate definition should capture this element,

without omitting the insight already noted that safety judgments are relative to people's value perspectives (Council for Science and Society, 1977, 13).

We propose to adopt as our working definition a modified version of Lowrance's definition:

> A thing is safe if, were its risks fully known, those risks would be judged acceptable in light of settled value principles.

More fully,

> A thing is safe (to a certain degree) with respect to a given person or group at a given time if, were they fully aware of its risks and expressing their most settled values, they would judge those risks to be acceptable (to a certain degree).

The objections to Lowrance's definition raised by the examples given above are met by the new definition's "knowledge" condition. And the further condition that a judgment about safety express "settled value principles" helps to rule out as irrelevant many other types of judgments that could be problematic: For example, judgments made while heavily intoxicated would not count.

Thus in our view safety is a matter of how people *would* find risks acceptable or unacceptable *if* they knew the risks and were basing their judgments on their most settled value perspectives. To this extent safety is an *objective* matter. It is a *subjective* matter to the extent that value perspectives differ. In what follows we will usually speak of safety simply as acceptable risk. But this is merely for convenience, and should be interpreted as an endorsement of Lowrance's definition only as we have qualified it.

Safety is frequently thought of in terms of degrees and comparisons. We speak of something as "fairly safe" or "relatively safe" (compared with similar things). Using our definition, this translates as the degree to which a person or group, judging on the basis of their settled values, would decide that the risks of something are more or less acceptable in comparison with the risks of some other thing. For example, when we say that airplane travel is safer than automobile travel, we mean that for each mile traveled it leads to fewer deaths and injuries—the risky elements which our settled values lead us to avoid.

We interpret "things" to include products as well as services, institutional processes, and disaster protection. The definition could therefore be extended to medicine, finance, and international affairs, to mention just a few of the "things" and "services" organized by people. And for engineers the definition would extend to the safe operation of systems and the prevention of natural or people-caused disasters.

Risks

We say a thing is "not safe" if it exposes us to unacceptable danger or hazard. What is meant by "risk"? *A risk is the potential that something unwanted and*

harmful may occur. We take a risk when we undertake something or use a product or substance that is not safe. Rowe refers to the "potential for the realization of unwanted consequences from impending events" (Rowe, 1977, 24). Thus a future, possible, occurrence of harm is postulated.

Risk, like harm, is a broad concept covering many different types of unwanted occurrences. In regard to technology, it can equally well include dangers of bodily harm, of economic loss, or of environmental degradation. These in turn can be caused by delayed job completion, faulty products or systems, and economically or environmentally injurious solutions to technological problems.

Good engineering practice has always been concerned with safety. But as technology's influence on society has grown, so has public concern about technological risks increased. In addition to measurable and identifiable hazards arising from the use of consumer products and from production processes in factories, some of the less obvious effects of technology are now also making their way to public consciousness. And while the latter are often referred to as "new risks," many of them have existed for some time. They are new only in the sense that (1) they are now identifiable (because of changes in magnitude of the risks they present, having passed a certain threshold of accumulation in our environment, or because of a change in measuring techniques, allowing detection of hitherto unnoticeable traces), or (2) the public's perception of them has changed (because of education, experience, or media attention, or because of a reduction in other hitherto dominant and masking risks).

Meanwhile, natural hazards continue to threaten human populations. Technology has greatly reduced the scope of some of these, such as floods, but at the same time it has increased our vulnerability to others as they affect our ever greater concentrations of population and cause greater damage to our finely tuned technological networks.

A word here should be said about disasters. A disaster does not take place until a seriously disruptive event coincides with a state of insufficient preparedness (Dynes, 1970). Hence the *Titanic*'s collision with an iceberg did not in itself constitute a disaster, but rather an emergency. The real disaster in terms of lives lost came about because emergency preparedness was inadequate. There were too few lifeboats, and there had been no lifeboat drills worth mentioning.

And if a disaster emerges from a combination of factors, so too does a risk—in the latter case from a combination of probability and consequence. The probabilistic aspects arise out of uncertainties over the event and who its victims will be, and the severity of the risk is judged by its nature and possible consequences (Rowe, 1977, 28). All this, of course, is related to the notion of experiment, for we are speaking of the "experimental" risks connected with the introduction of new technology, the risks associated with new applications of familiar technology, and the risks arising from attempts

at disaster control. So again we shall find our paradigm of engineering as social experimentation to be of some use as we unravel the ethical implications of safety and risk in regard to engineered products.

Acceptability of Risk

Having adopted a modified version of Lowrance's definition of safety as acceptable risk, we need to examine the idea of acceptability more closely. William D. Rowe says that "a risk is acceptable when those affected are generally no longer (or not) apprehensive about it" (Rowe, 1979, 328). Apprehensiveness depends to a large extent on how the risk is perceived. This is influenced by such factors as whether or not the risk is assumed voluntarily; the effects of knowledge on how the probabilities of harm (or benefit) are perceived; job-related or other pressures that cause people to be aware of or (alternatively) to overlook risks; whether or not the effects of a risky activity or situation are immediately noticeable or are close at hand; and whether or not the potential victims are identifiable beforehand. Let us illustrate these elements of risk perception by means of some examples.

Voluntarism and Control John and Ann Smith and their children enjoy riding motorcycles over rough terrain for amusement. They take *voluntary* risks—that is part of being engaged in such a potentially dangerous sport. They do not expect the manufacturer of their dirt bikes to adhere to the same standards of safety as they would the makers of a passenger car used for daily commuting. The bikes should be sturdy, but guards covering exposed parts of the engine, padded instrument panels, collapsible steering mechanisms, or emergency brakes are clearly unnecessary, if not inappropriate.

In discussing dirt bikes and the like we do not include the all-terrain three-wheel vehicles. Those represent hazards of greater magnitude because of the false sense of security they give the rider. They tip over easily. During the 5 years before they were forbidden in the United States, they were responsible for nearly 900 deaths and 300,000 injuries. About half of the casualties were children under 16.

John and Ann live near a chemical plant. It is the only area in which they can afford to live, and it is near the shipyard where they both work. At home they suffer from some air pollution, and there are some toxic wastes in the ground. Official inspectors tell them not to worry. Nevertheless they do, and they think they have reason to complain—they do not care to be exposed to risks from a chemical plant with which they have no relationship except on an involuntary basis. Any beneficial link to the plant through consumer products or other possible connections is very remote and, moreover, subject to choice.

John and Ann behave as most of us would under the circumstances: We are much less apprehensive about the risks to which we expose ourselves

voluntarily than those to which we are exposed involuntarily. "We are loath to let others do unto us what we happily do to ourselves" (Starr, quoted in Lowrance, 1976, 87). In terms of our "engineering as social experimentation" paradigm, people are more willing to be the subjects of their own experiments (social or not) than of someone else's.

Intimately connected with this notion of voluntarism is the matter of *control*. The Smiths choose where and when they will ride their bikes. They have selected their machines and they are proud of how well they can control them (or think they can). They are aware of accident figures, but they tell themselves those apply to other riders, not to them. In this manner they may well display the characteristically unrealistic confidence of most people when they believe hazards to be under their control (Slovic, Fischhoff, and Lichtenstein, April 1979, June 1980, and May 1979). But still, riding motorbikes cross-country, skiing, hanggliding, horseback riding, boxing, and other hazardous sports are usually carried out under the implied control of the participants, which is a good part of why they are engaged in voluntarily at all and why their enthusiasts worry less about their risks than the dangers of, say, air pollution or airline safety. Another reason for not worrying so much about the consequences of these sports is that rarely does any one accident injure any appreciable number of innocent bystanders.

Effect of Information on Risk Assessments The manner in which information necessary for decision making is presented can greatly influence how risks are perceived. The Smiths are careless about using seat belts in their car. They know that the probability of their having an accident on any one trip is infinitesimally small. Had they been told, however, that in the course of 50 years of driving, at 800 trips per year, there is a probability of 1 in 3 that they will receive at least one disabling injury, their seat belt habits (and their attitude about seat belt laws) would likely be different (Arnould, 1981, 35).

Studies have verified that a change in the manner in which information about a danger is presented can lead to a striking reversal of preferences about how to deal with that danger. Consider, for example, an experiment in which two groups of around 150 people each were told about the strategies available for combatting a disease. The first group was given the following description:

> Imagine that the U.S. is preparing for the outbreak of an unusual Asian disease, which is expected to kill 600 people. Two alternative programs to combat the disease have been proposed. Assume that the exact scientific estimate of the consequences of the programs are as follows:
>
> If Program A is adopted, 200 people will be saved....
>
> If Program B is adopted, there is ⅓ probability that 600 people will be saved, and ⅔ probability that no people will be saved....
>
> Which of the two programs would you favor? (Tversky and Kahneman, 1981, 453)

The researchers reported that 72 percent of the respondents selected Program A, and only 28 percent selected Program B. Evidently the vivid prospect of saving 200 people led many of them to feel averse to taking a risk on possibly saving all 600 lives.

The second group was given the same problem and the same two options, but the options were worded differently:

> If Program C is adopted 400 people will die....
>
> If Program D is adopted there is ⅓ probability that nobody will die, and ⅔ probability that 600 people will die....
>
> Which of the two programs would you favor? (Tversky and Kahneman, 1981, 453)

This time only 22 percent chose Program C, which is the same as Program A. 78 percent chose Program D, which is identical to Program B.

One conclusion that we draw from the experiment is that options perceived as yielding firm gains will tend to be preferred over those from which gains are perceived as risky or only probable. A second conclusion is that options emphasizing firm losses will tend to be avoided in favor of those whose chances of success are perceived as probable. In short, people tend to be more willing to take risks in order to avoid perceived firm losses than they are to win only possible gains.

The difference in perception of probable gain and probable loss is illustrated graphically in Fig. 4-1. The typical risk-benefit value function shown there drops more steeply on the loss portion than it rises on the gain portion. We have included on this graph a loss side threshold, as does Rowe (Rowe, 1979, 331). The threshold is ascribable to the human habit of ignoring smaller hazards in order to avoid anxiety overload and means that no value is attached to a first small amount of loss or that no effort is expended to overcome the loss. We have added a similar, though smaller, threshold on the gain side to account for the normal human inertia and a certain amount of inherent generosity that often restrain people in how they set about seeking their own gain.

The thresholds are significant because they remind us that different people have different tolerances for specific conditions. Someone with a respiratory illness, for example, will react to the smallest amount of air pollution; thus the threshold for pollution is near zero for that person. An entire population living near an oil refinery, however, will have a fairly high tolerance (i.e., a large threshold) as far as automobile emissions alone are concerned.

Job-Related Risks John Smith's work in the shipyard has in the past exposed him to asbestos. He is aware now of the high percentage of asbestosis cases among his coworkers, and after consulting his own physician was told that he was slightly affected himself. Even Ann, who works in a clerical position at the shipyard, has shown symptoms of asbestosis as a result of handling her husband's clothes. Earlier John saw no point to "all the fuss stirred

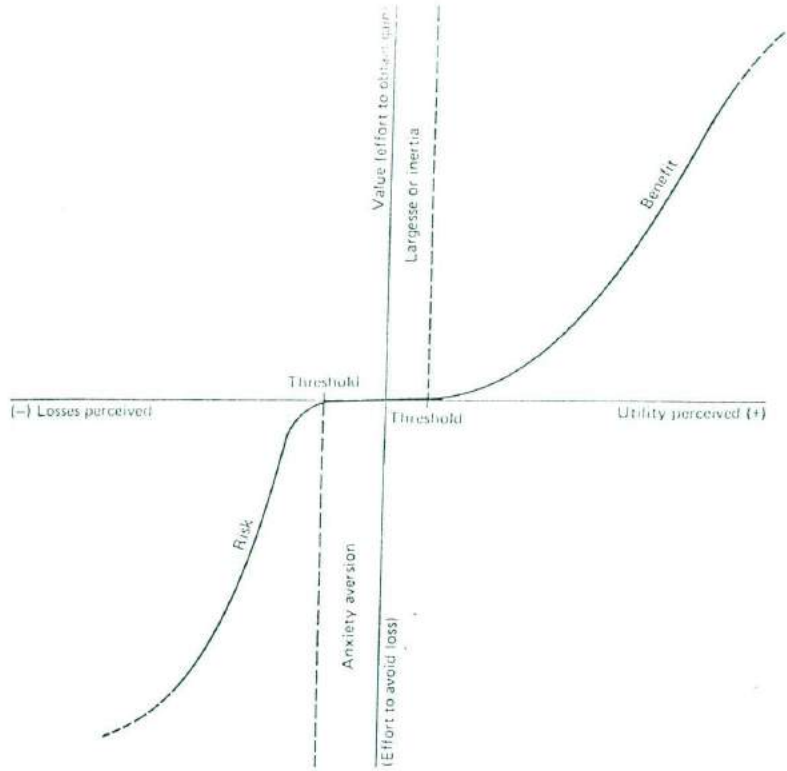


FIGURE 4-1
Typical risk-benefit value function.

up by some do-gooders." He figured that he was being paid to do a job, he felt the masks which were handed out occasionally gave him sufficient protection, and he thought the company physician was giving him a clean bill of health.

In this regard John's thinking is similar to that of many workers who take risks on their jobs in stride, and sometimes even approach them with a bravado attitude. Of course exposure to risks on a job is in a sense voluntary since one can always refuse to submit oneself to them, and workers perhaps even have some control over how their work is carried out. But often employees have little choice other than to stick with what is for them the only available job and to do as they are told. What they are often not told about is their hidden exposure to toxic substances and other dangers. Unions and occupational health and safety regulations (such as right to know rules regard-

ing toxics) can correct the worst situations, but standards regulating conditions in the workplace (its air quality, for instance) are generally still far below those which regulate conditions in our general (public) environment. It may be argued that the "public" encompasses many people of only marginal health whose low thresholds for pollution demand a fairly clean environment. On the other hand factory workers are seldom carefully screened for their work. And in all but the most severe environments (those conducive to black lung or brown lung, for instance), unions display little desire for change lest necessary modifications of the workplace force employers out of business altogether.

Engineers who design and equip work stations must take into account the cavalier attitude toward safety shown by many workers, especially when their pay is on a piecework basis. And when one worker complains about unsafe conditions, but others do not, the complaint should not be dismissed as coming from a crackpot. Any report regarding unsafe conditions merits serious attention.

Pilot Dan Gellert's reports about problems with the L-1011s should have been looked into promptly. Later attempts to discredit him through psychiatric examinations may have been used partly as a legal ploy, but management might also have found it hard to believe that anyone could be so particular about safety. And yet Gellert was properly concerned about his responsibilities as a pilot—and all the more so because he had an airliner full of passengers and crew relying on his skill and the integrity of the plane rather than just himself to take into consideration. Which brings us to yet another factor that colors our perception of risks: their magnitude and proximity.

Magnitude and Proximity Our reaction to risk is affected by the *dread* of a possible mishap, both in terms of its magnitude and of the personal identification or relationship we may have with the potential victims. A single major airplane crash, the specter of a child we know trapped in a cave-in—these affect us more acutely than the ongoing but anonymous carnage on the highways, at least until someone close to us is killed in a car accident.

In terms of numbers alone we feel much more keenly about a potential risk if one of us out of a group of 20 intimate friends is likely to be subjected to great harm than if it might affect, say, 50 strangers out of a larger group of 1000. This proximity effect is noticeable in the time domain as well. A future risk is easily dismissed by various rationalizations including (1) the attitude of "out of sight, out of mind," (2) the assumption that predictions for the future must be discounted by using lower probabilities, or (3) the belief that a countermeasure will be found in time.

The numbers game can easily make us overlook losses which are far greater than the numbers would reveal by themselves. Consider the 75 men lost when the unfinished Quebec Bridge collapsed in 1907. As William Starna relates,

> Of those 75 men, no fewer than 35 were Mohawk Indians from the Caughnawaga Reserve in Quebec. Their deaths had a devastating effect on this small Indian community, altering drastically its demographic profile, its economic base, and its social fabric. Mohawk steelworkers would never again work in such large crews, opting instead to work in small groups on several jobs. Today, Mohawk high-steelworkers remain among the highest regarded and most skilled in their field (Starna, 1986).

Two other examples which involved large-scale disruptions of communities were mentioned earlier: the Buffalo Creek flood (Study Question 4, p. 102.) and Bhopal (discussed in Chap. 7). The forceful evacuation of Pripyat next to the Chernobyl nuclear power plant is part of the story of the reactor failure discussed later in this chapter.

Lessons for the Engineer

Engineers in their work face two problems in regard to public conceptions of safety. On the one hand there is the overoptimistic attitude that things which are familiar, which have not hurt us before, and over which we have some control, present no real risks. On the other hand is the dread people feel when accidents kill or maim in large numbers or harm those we know, even though statistically speaking such accidents might occur infrequently.

Leaders of industry are sometimes heard to proclaim that those who fear the effects of air pollution, toxic wastes, or nuclear power are emotional and irrational or politically motivated. This in our view is a misperception of legitimate concerns expressed publicly by thoughtful citizens. It is important that engineers recognize as part of their work reality such widely held perceptions of risk and take them into account in their designs. It is not wise to proceed under the assumption that "education" will quickly change the public's underestimation or overestimation of risk. As Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein point out:

> Another barrier to educational attempts is that people's beliefs change slowly and are extraordinarily resistant to new information. Research in social psychology has often demonstrated that once formed, people's initial impressions tend to structure the way they interpret subsequent information. They give full weight to evidence that is consistent with their initial beliefs while dismissing contrary evidence as unreliable, erroneous, or unrepresentative. Whereas opponents of nuclear power believe the accident at Three Mile Island "proved" how dangerous reactors are, proponents felt that it confirmed their faith in the effectiveness of the multiple safety and containment system (Slovic, Fischhoff, and Lichtenstein, 1980, 48).

And in regard to professionals they continue:

> Since even well-informed citizens have difficulty in judging risk accurately, and the cognitive functioning of experts appears to be basically like that of everyone else, it seems clear that no one person or profession knows how to get the right answers. The best we can hope to do is to keep the particular kinds of mistakes to

which each of us is prone to a minimum by being more aware of our tendency to make mistakes (Slovic, Fischhoff, and Lichtenstein, 1980, 48).

Finally, in regard to wisdom over which no one holds a monopoly, Slovic writes:

> Perhaps the most important message from this research [on risk perception] is that there is wisdom as well as error in public attitudes and perceptions. Lay people sometimes lack certain information about hazards. However, their basic conceptualization of risk is much richer than that of experts and reflects legitimate concerns that are typically omitted from expert risk assessments. As a result, risk communication and risk management efforts are destined to fail unless they are structured as a two-way process. (Slovic, 1987)

Study Questions

1 Describe a real or imagined traffic problem in your neighborhood involving children and elderly people who find it difficult to cross a busy street. Put yourself in the position of (*a*) a commuter traveling to work on that street, (*b*) the parent of a child, or the relative of an older person, who has to cross that street on occasion, (*c*) a police officer assigned to keep the traffic moving on that street, and (*d*) the town's traffic engineer working under a tight budget.

Describe how in these various roles you might react to (*i*) complaints about conditions dangerous to pedestrians at that crossing and (*ii*) requests for a pedestrian crossing protected by traffic lights.

2 In some technologically advanced nations, a number of industries which have found themselves restricted by safety regulations have resorted to dumping their products on, or moving their production processes to, less-developed countries where higher risks are tolerated. Examples are the dumping of unsafe or ineffective drugs on the Third World by pharmaceutical companies from Western Europe, communist bloc countries, Japan, and the United States (Silverman, Lee, and Lydecker, 1981) and the transfer of asbestos processing from the United States to Mexico (Shue, 1981, 586). To what extent do differences in perception of risk justify the transfer of such merchandise and production processes to other countries? Is this an activity that can or should be regulated?

3 The industrial accident described below and illustrated in Fig. 4-2 raises several issues of ethical import. Identify and discuss them.

> *The following news story is based on the Nassau edition of* Newsday, *the Long Island, N.Y., newspaper, April 24, 1981.*
>
> Inadequate safety precautions and an accident inside an empty water tank caused the deaths of two workmen in New Jersey on April 23. At 4 p.m., a scaffold inside the tank collapsed and caused the two men painting the tank to fall to the bottom. Stranded there, they were overcome by paint fumes and eventually lost consciousness. John Bakalopoulos, 34, of Brooklyn, N.Y. and Leslie Salomon, 31, also of Brooklyn, were not wearing oxygen masks. The Suffolk County Water Authority's contract for the painting job specified that workmen wear "air hoods," masks connected to air compressors. The masks were available, but Bakalopoulos and Salomon had decided not to wear them because they

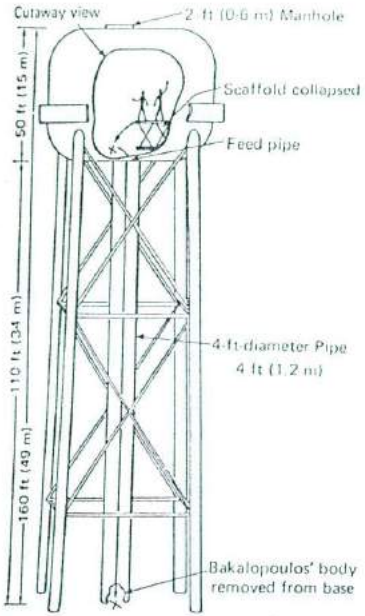


FIGURE 4-2
Accident in a water tank. (*Source:* Opflow, *American Water Works Association, vol. 7, no. 6, June 1981, p. 3, using material from* Newsday, *Nassau edition, Long Island, New York, April 24, 1981.*)

were unwieldy. Instead, Bakalopoulos wore a thin gauze mask designed to filter out dust and paint particles. Salomon wore no mask.

Peter Koustas, the safety man who was handling the compressor and paint feed outside the tank, asked a nearby resident to call firemen as soon as he realized the scaffold had collapsed. Then he rushed into the tank with no oxygen mask, and he, too, was overcome by the fumes and lost consciousness.

The men lay unconscious for hours as rescue efforts of more than 100 policemen, firemen, and volunteers were hampered by bad weather. Intense fog, rain, and high winds made climbing the tank difficult and restricted the use of machinery. Several men collapsed from fatigue.

Inside the tank, conditions were worse. Because of the heavy fumes, rescuers used only hand-held, battery-powered lights, fearing that sparks from electric lights might cause an explosion. Lt. Larry Viverito, 38, a Centereach, N.Y. volunteer fireman, was overcome by fumes 65 ft (20 m) above the floor of the tank. Fellow rescuers had to pull him out.

Rescuer John Flynn, a veteran mountain climber, said he hoped he would never have to go through anything like that night again. For five hours he set up block-and-tackle pulleys, tied knots, adjusted straps on stretchers, and attached safety lines and double safety lines. The interior of the tank was as blindingly white as an Alpine blizzard—completely and nauseatingly disorienting. Fans that had been set up to pull fresh air into the tank caused deafening noise.

When Flynn first reached the tank floor, he stepped into the wet paint and be-

gan to slide toward the uncovered 4-ft (1.2-m) opening to the feeder pipe in the center of the floor. Flynn was able to stop sliding, but John Bakalopoulos wasn't as fortunate.

As rescuers watched helplessly, Bakalopoulos, still out of reach, stirred, rolled over, and in the slippery paint slid into the feeder pipe. He plunged 110 ft (34 m) to the bottom.

Bakalopoulos was dead on arrival at the University Hospital in Stony Brook, N.Y. Peter Koustas, rescued at 1:45 a.m. and suffering from hypothermia, died the following morning when his heart failed and he could not be revived. Only Leslie Salomon survived. (*Quoted with permission from* Opflow, *Am. Water Works Assoc., vol. 7, no. 6, June 1981, p. 3, and from* Newsday.)

4 Grain dust is pound for pound more explosive than coal dust or gunpowder. Ignited by an electrostatic discharge or other causes, it has ripped apart grain silos and killed or wounded many workers over the years. When fifty-four people were killed during Christmas week 1977, grain handlers and the U.S. government finally decided to combat dust accumulation (Marshall, 1983). Ten years, 59 deaths, and 317 serious injuries later, a compromise standard has been agreed upon which designates dust accumulation of ⅛ inch or more as dangerous and impermissible. Use grain facility explosions for a case study of workplace safety and rule making.

5 The oil rig *Alexander L. Kielland* collapsed during a storm, taking 122 men to their deaths. The structure was weak because of a faulty weld. So many men died because it was difficult to launch the lifeboats. Search the literature (you may start with a chapter on the *Kielland* in Bignell and Fortune, 1984), then assess the hazards of working and living on an oil rig in the North Sea, with special emphasis on the opportunities for safe escape.

ASSESSMENT OF SAFETY AND RISK

Absolute safety is not attainable, and any improvement in safety as it relates to an engineered product is often accompanied by an increase in cost of that product. On the other hand, products that are not safe incur secondary costs to the manufacturer beyond the primary (production) costs that must also be taken into account—costs associated with warranty expenses, loss of customer goodwill and even loss of customers due to injuries sustained from use of the product, litigation, possible downtime in the manufacturing process, and so forth. It is therefore important for manufacturers and users alike to reach some understanding of the risks connected with any given product and of what it might cost to reduce those risks or not reduce them.

As Fig. 4-3 indicates, an emphasis on high safety (low risks) leads to high primary costs, but secondary costs are low. At the other extreme of high risks (low safety), one saves on primary costs but pays dearly because of high secondary costs. In between, where the slopes of the primary and secondary cost curves are equal, is the point of minimum total cost. If all costs were quantifiable, that optimum point would be the goal to reach for. But before we crank up our computers to home in on such an optimal design, we must be clear about how to determine risk (to be discussed in this section) and how to compare losses with benefits (to be covered in the next section).

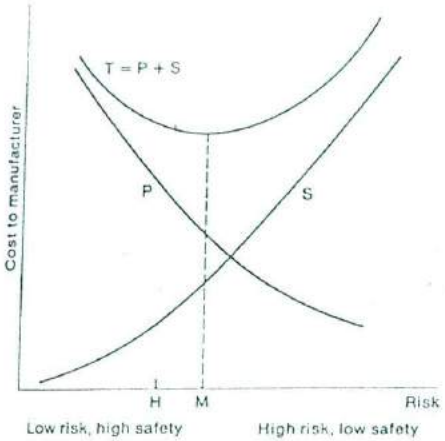


FIGURE 4-3
Why both low-risk and high-risk products are costly. P = primary cost of product, including cost of safety measures involved; S = secondary costs, including warranties, loss of customer goodwill, litigation costs, costs of down time, and other secondary costs. T = total cost. Minimum total cost occurs at M, where incremental savings in primary cost (slope of P) are offset by an equal incremental increase in secondary cost (slope of S). Highest acceptable risk (H) may fall below risk at least cost (M), in which case H and its higher cost must be selected as design or operating point.

Knowledge of Risk

One would think that experience and historical data would provide good information about the safety of standard products. Much has been collected and published; gaps remain, however, because (1) there are some industries where information is not freely shared, and (2) there are always new applications of old technology which render the available information less useful.

Engineers are by nature inclined to share information freely. It is in this spirit, according to R. R. Whyte in *Engineering Progress through Trouble*, that Robert Stephenson, famous bridge builder during the first half of the nineteenth century, took the following position upon reviewing a technical paper:

> ...he hoped that all the casualties and accidents, which had occurred during their progress, would be noticed in revising the paper; for nothing was so instructive to the younger Members of the Profession, as records of accidents in large works, and of the means employed in repairing the damage. A faithful account of those accidents, and of the means by which the consequences were met, was really more valuable than a description of the most successful works. The older Engineers derived their most useful store of experience from the observations of those casualties which had occurred to their own and to other works, and it was most important that they should be faithfully recorded in the archives of the Institution (R. R. Whyte, 1975, v).

We also take the following account from pp. 54–57 of the same book: In 1950 the chief engineer for a British manufacturer of large generators invited his competitors to study the failure of a rotor endbell during overspeed tests. The endbell is a retaining sleeve which holds in place the endturns of the

rotor winding so they will not fly apart at the high speed of the turbine generator. Because the endbell has to be made of nonmagnetic steel, it presents severe metallurgical problems. This engineer's action led to a similar frank divulgence of information on the occasion of another, similar, failure in Canada some years later.

Such examples are noteworthy because they are so rare—which is regrettable. Too many companies believe that releasing technical information might hurt their competitive position, if not place them at a disadvantage in case of litigation. So it is that new engineers and new companies usually have to learn from scratch, although sometimes past experience is used effectively to educate beginners (see, for example, the textbook on soil mechanics and foundations, *Introductory Soil Mechanics and Foundations*, by George B. Sowers and George F. Sowers, 1970).

Uncertainties in Design

Risk is seldom intentionally designed into a product. It arises because of the many uncertainties faced by the design engineer, the manufacturing engineer, and even the sales and applications engineer.

To start with, there is the purpose of a design. Let us consider an airliner. Is it meant to maximize profits for the airline, or is it intended to give the highest possible return on investment? The answer to that question is important to the company because on it hinge different decisions and their outcomes and the possibility of the airline's economic success or ruin. Investing $50 million in a jumbo jet to bring in maximum profits of, say, $10 million during a given time period involves a lower return on investment than spending $24 million on a medium-sized jet to bring in a return of $6 million in that same period.

Regarding applications, designs which do quite well under static loads may fail under dynamic loading. A famous example is the wooden bridge that collapsed when a contingent of Napoleon's army crossed it marching in step. This even affected one of Robert Stephenson's steel bridges, which shook violently under a contingent of marching British troops. Ever since then, soldiers are under orders to fall out of step when crossing a bridge. Wind can also cause severe vibrations: The Tacoma Narrows Bridge, which collapsed some years ago, and a high tension power line across the Bosphorus that broke after a short circuit caused by swinging cables are but two examples.

Apart from uncertainties about applications of a product, there are uncertainties regarding the materials of which it is made and the quality of skill that goes into designing and manufacturing it. For example, changing economic realities or hitherto unfamiliar environmental conditions such as extremely low temperatures may affect how a product is to be designed. A typical "handbook engineer" who extrapolates tabulated values without regard to their implied limits under different conditions will not fare well under such circumstances. Even a careful analyst will face difficulties when con-

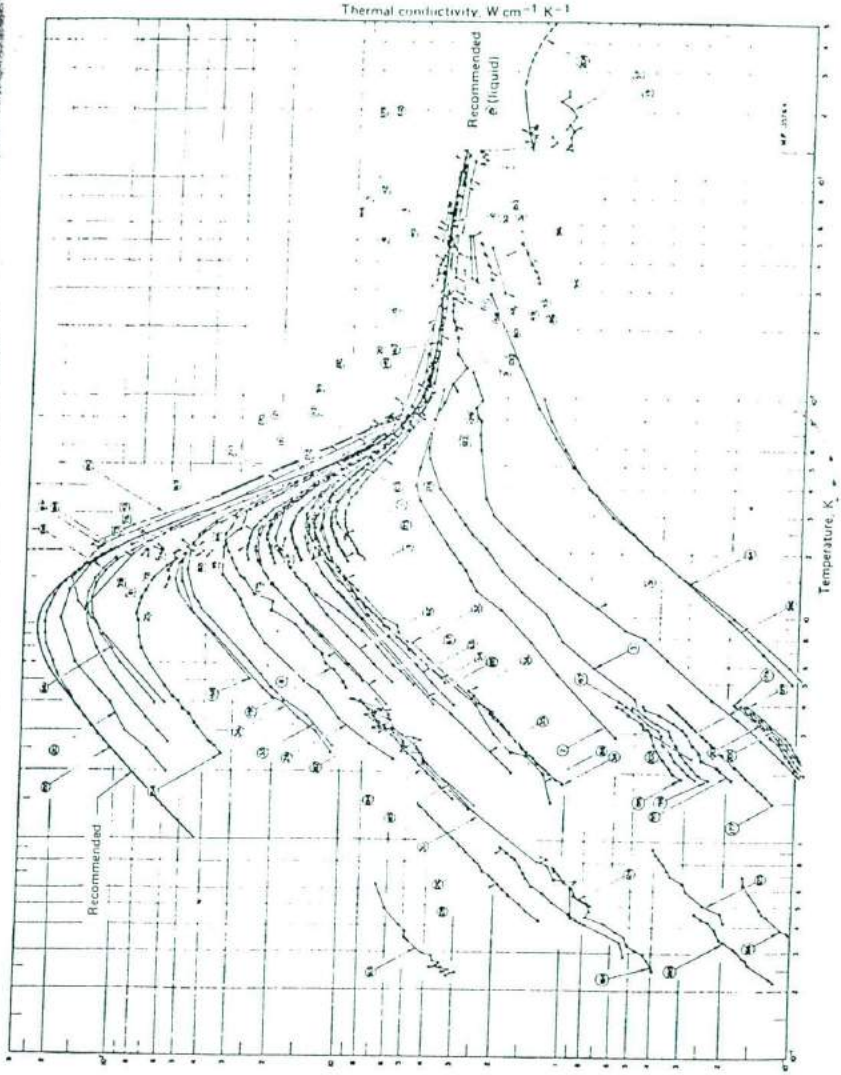


FIGURE 4-4
Thermal conductivity of copper over wide ranges of temperature as observed by different investigators—an example of the diversity in test results that can affect engineering decisions about safety. (*From D. R. Lide, Jr., "Critical Data for Critical Needs,"* Science, *vol. 212, June 19, 1981, p. 1344.*)

fronted with data such as those illustrated in Fig. 4-4, which gives the thermal conductivity of copper over wide ranges of temperature as observed by different investigators.

Caution is required even with standard materials specified for normal use. In 1981 a new bridge that had just replaced an old and trusted ferry service across the Mississippi at Praire du Chien, Wisconsin, had to be closed because 11 of the 16 flange sections in both tie girders were found to have been fabricated from excessively brittle steel (ENR, 1981). In the meantime, the ferries had disappeared! While strength tests are routinely carried out on concrete, the strength of steel is all too often taken for granted.

Such drastic variations from the standard quality of a given grade of steel are rather exceptional. More typically the variations are small. Nevertheless the design engineer should realize that the supplier's data on items like steel, resistors, insulation, optical glass, and so forth apply to statistical averages only. Individual components can vary considerably from the mean.

Engineers traditionally have coped with such uncertainties about materials or components, as well as incomplete knowledge about the actual operating conditions of their product, by introducing a comfortable "factor of safety." That factor is intended to protect against problems arising when stresses due to anticipated loads (duty) and stresses the product as designed is supposed to withstand (strength or capability) depart from their expected values. Stresses can be of a mechanical or any other nature—for example, an electric field gradient to which an insulator is exposed, or the traffic density at an intersection.

A product may be said to be safe if its capability exceeds its duty. But this presupposes exact knowledge of actual capability and actual duty. In reality the stress calculated by the engineer for a given condition of loading and the stress which ultimately materializes at the loading may vary quite a bit. This is because each component in an assembly has been allowed certain tolerances in its physical dimensions and properties—otherwise the production cost would be prohibitive. The result is that the assembly's capability as a whole cannot be given by a single numerical value but must be expressed as a probability density which can be graphically depicted as a "capability" curve (see Fig. 4-5*a* and *b*). For a given point on a capability curve, the value along the vertical axis gives the probability that the capability, or strength, is equal to the corresponding value along the horizontal axis.

A similar curve can be constructed for the duty which the assembly will actually experience. The stress exposure varies because of differences in loads, environmental conditions, or the manner in which the product is used. Associated with the capability and duty curves are nominal or, statistically speaking, expected values C and D. We often think and act only in terms of nominal or expected values. And with such a deterministic frame of mind, we may find it difficult to conceive of engineering as involving experimentation. The "safety factor" C/D rests comfortably with our consciences. But how sure can we be that our materials are truly close to their specified

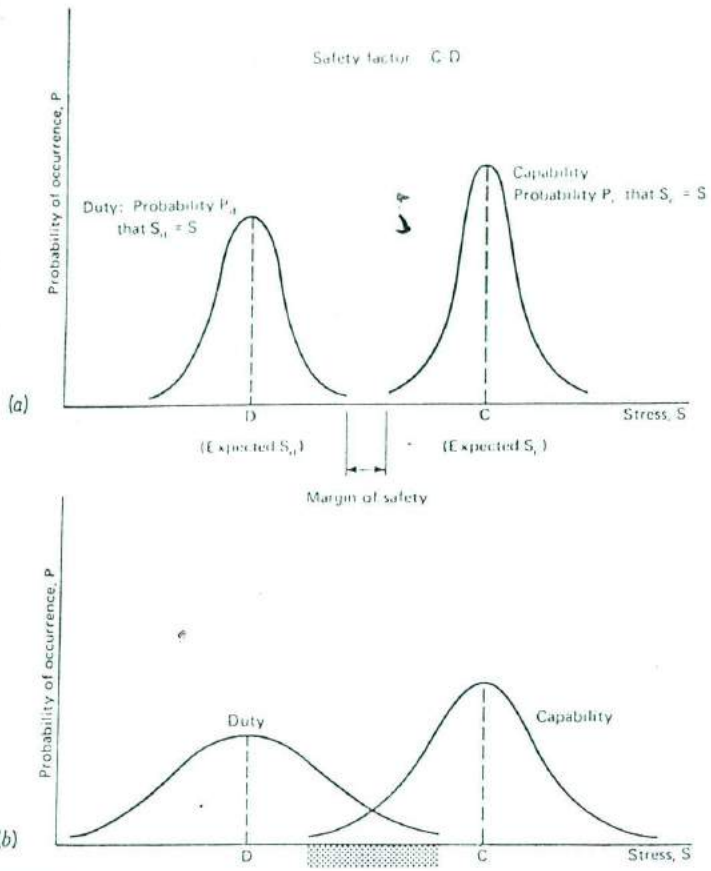


FIGURE 4-5
Probability density curves for stress in an engineered system (*a*) Variability of stresses in a relatively safe case. (*b*) An unsafe case (danger is due to some probable overlap in duty and capability stresses).

nominal properties? Or that the loads will not vary too widely from their anticipated values or occur in environments hostile to the proper functioning of the materials? It is entirely conceivable that the capability and duty curves will assume flatter shapes because of increased variances (see Fig. 4-5*b*) than they would have under normal conditions, as in Fig. 4-5*a*. And Fig. 4-5*b* shows how it is probable that load stress may exceed design stress along the shaded region of stress. Mathematical treatment of this topic is offered by,

among others, Edward B. Haugen, who reminds his readers how "the safety factor concept completely ignores the facts of variability that result in different reliabilities for the same safety factor" (Haugen, 1968, 5).

A more appropriate measure of safety would be the "margin of safety," which is shown in Fig. 4-5*a*. If it is difficult to compute such a margin of safety for ordinary loads used every day, imagine the added difficulties that arise when repeatedly changing loads have to be considered. As F. Nixon, N. E. Frost, and K. J. March point out:

> The use of a general safety margin on the static strength of a material (or structure) is quite unsuitable for cyclic loadings. For example, local static stresses are usually unimportant in ductile materials because regions which become overstressed may yield, with the result that the stress becomes more uniformly distributed. However, when the loading is cyclic, yield can affect only the mean value of the local stresses to which any local discontinuities give rise. Thus, the merit of a structure subjected to dynamic loadings depends to a great extent on the skill of the designer in avoiding unnecessary concentrations of stress (Nixon, Frost, and March, 1975, 137).

Testing for Safety

The widely proclaimed "safety factor" thus obviously has some serious conceptual flaws. So what can the engineer do to assure safety? "Rely on experience" was mentioned at the outset of this discussion. But it was also pointed out that experience gained by one engineer is all too often not passed on to others, especially if the experience was professionally embarrassing. Bad news travels fast, we agree, but usually it travels unaccompanied by hard facts.

Another way of gaining experience is through tests. Under certain conditions this can be a valuable source of information, especially if the testing of materials or a product is carried out to destruction. An example of such testing was that performed on a Comet aircraft fuselage after two of those early jets had crashed in service in 1954. One conclusion emerged from initial investigations:

> ...fatigue of the pressure cabin. The only possible objection was that fatigue so early in the lives of the two aircraft seemed at that time incredible. These arguments provided the justification and the objective for the experimental attack that then followed.
>
> The fatigue-testing of a complete full-size pressure cabin and fuselage went beyond anything ever before attempted. For safety, water was used as the testing medium, and the whole fuselage was immersed in a 250,000 gal. tank.
>
> It was clearly necessary to introduce every conceivable adverse factor in addition to pressure. In particular, the wings had to be included in the test and given the appropriate load fluctuations. Total immersion of the wings was considered, but rejected in favor of their projecting through the sides of the tank, the water being held back by flexible sleeves that allowed the wings to articulate.
>
> With [special apparatus] the cabin was made to breathe in and out as the wings

were forced to bend up and down realistically. The test went on night and day until a piece of pressure cabin 20 ft^2 in area was pushed out almost instantaneously. The failure was initiated by a fatigue crack at a corner of one of the forward windows. In the air, of course, this would have meant an explosion (De Havilland and Walker, 1975, 53).

The reader should note that this test was carried out *after* real accidents had occurred. The more usual procedure is to subject prototypes to testing. Yet there are severe limitations to relying on prototype tests, as R. R. Whyte points out:

> ...successful prototype testing and prolonged test-bed running also do not ensure a reliable machine.... Like the designer, the development engineer is seldom allowed sufficient time. In many cases all he has time for is a functional test too short to reveal potential weaknesses in the design such as a fatal resonant frequency, for example. In others all that is stipulated even by customers who should know better, is that a single prototype should satisfactorily pass a "type-approval test"; maybe a few hundred operations or hours of running.
>
> Such a test can do no more than demonstrate that one individual product—seldom representative of large quantities—is capable of passing the stipulated test. It can do little to demonstrate the ultimate capability of the design. It can do nothing to indicate the variability in capability which is likely to exist when numbers of similar products are to be produced or the long-term effects such as corrosion or fatigue (R. R. Whyte, 1975, 139).

In the case of the space shuttle *Challenger* the flights occurred outside the field joints' test envelope; extrapolation to performance at lower temperatures was based more on handbook material specifications than on available engineering judgment.

Even prototype tests and routine quality assurance tests are frequently not carried out properly. Suppliers of rifles and ammunition to the Armed Forces have been found to have committed fraud in the testing of their products; the Alaska pipeline was plagued with poor welds and inadequate testing; the Ford Motor Co. at one time was found to have falsified emission test data; the B. F. Goodrich Co. delivered an aircraft brake for test flights on a new Air Force plane although the brake failed to meet Air Force specifications even according to a common sense interpretation of those specifications; and bogus parts, indistinguishable from the originals in appearance but much lower in quality, are flooding the U.S. market.

In short, we cannot trust testing procedures uncritically. Time pressure, as we have said, is one factor contributing to shoddy testing. The boredom of routine that tempts one to quickly duplicate test data of a repetitive nature can be another. At times there is pressure from management to "fudge the data for now" since "by the time we get into production we will have ironed out the problem." And not to be overlooked is the problem of outright fraud, as when testers are bribed to pass faulty items or when no tester was on the job although testing was claimed to have been undertaken. Conscientious engineers had therefore better make occasional spot checks on their own un-

less the organization they work for operates an independent testing service free of production pressures.

When Testing Is Inappropriate

Not all products can be tested to destruction. In such cases a simulation which traces the outcome of one or more hypothetical, risky events should be applied. A common approach is *scenario analysis*, in which one starts from a given event, then studies the different consequences which might evolve from it. Another approach, known as *failure modes and effects analysis*, systematically examines the failure modes of each component, without, however, focusing on causes or interrelationships among the elements of a complex system. In contrast to this is the *fault-tree analysis* method, in which one proposes a system failure and then traces the events back to possible causes at the component level.

Of these several techniques, the fault-tree method can perhaps most effectively illustrate the disciplined approach required to capture as much as possible of everything that affects the proper functioning and safety of a complex system. Please note, however, that no safety analysis should be attempted without a thorough understanding of the physical aspects of the system under study; the mere use of ready-made computer programs does not suffice except to facilitate intermediate calculations.

To illustrate the use of the fault-tree technique we resort to a rather simple example, a water system without filtration plant, depicted in Fig. 4-6. A fault tree for that water system is shown in Fig. 4-7. We start with the system failure at the top and work down to failures in various subsystems, components, and outside factors or events which could have given rise to the problem. Each level in the tree lists events that could have caused the problem listed in the level above it. "Could have" implies that one *or* more events could be the cause for the event at the next higher level. Sometimes one *and* another event—perhaps several events—must all occur for that next event to happen. Thus there are two types of logical statements that appear on the chart, OR and AND.

The fault tree in Fig. 4-7 has not been completed. There are several further levels which could be indicated. There are also possible omissions at the levels shown. But even though incomplete, this fault tree can give us a good qualitative sense of the types of risks to which the water system is exposed. Some analysts proceed further and attach probability figures to each event. The accuracy of such figures is always problematic, however, particularly when there is the chance of common-mode failures. An earthquake, for example, could damage not only the reservoir—it could cause any of the events in Fig. 4-7 trailed by the circled E, eventually affecting delivery of water. Say an earthquake causes crumbling of riverbanks and other damage leading to silting of the pump's source of water. If not properly filtered out, the silt

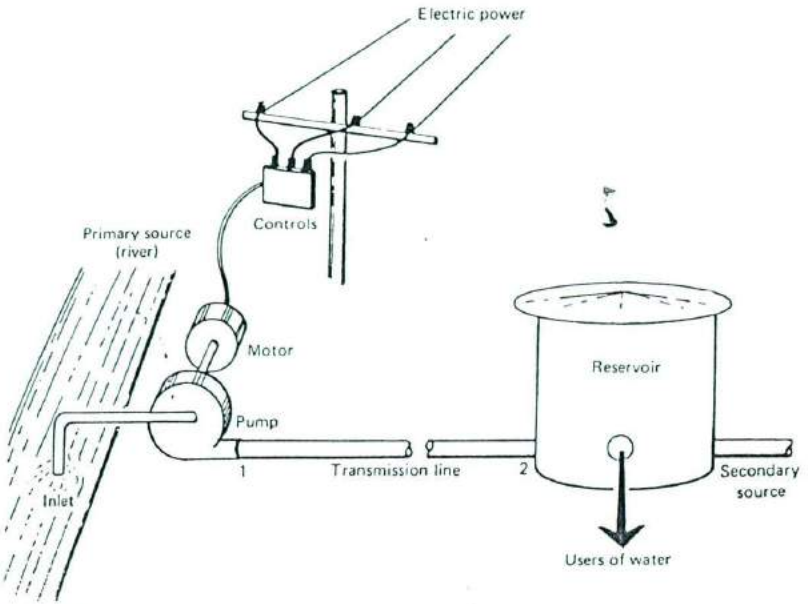


FIGURE 4-6
A simple water system.

could cause the impeller of the pump to wear out in no time at all. Alternatively the silting could cause the inlet to clog, thus stopping the inflow of water necessary to the pump's operation.

In the disaster that befell the passengers and the crew of the *Titanic*, the fact that the accident occurred at night certainly played its part as a "common-mode event" in producing the tragedy (Machol, 1975, 53). The iceberg could not be seen easily at night, the only radio operator on a nearby ship was asleep, and abandoning ship was more difficult at night than it would have been during the day. Thus because of the difficulty in foreseeing all common-mode events, one should treat the results of quantitative risk assessments with caution (see Study Question 4 below for a numerical example of this problem).

The strength of a fault-tree analysis lies in its qualitative aspects. It assists in the exposure of hitherto unforeseen situations. In a real-life water system analysis we would test for the availability of potable water and its usefulness. Water which is contaminated is not useful, even when available in large quantities at the householder's tap. Even high-quality water may not be useful when the sewer system is inoperative. On the other hand, even when no

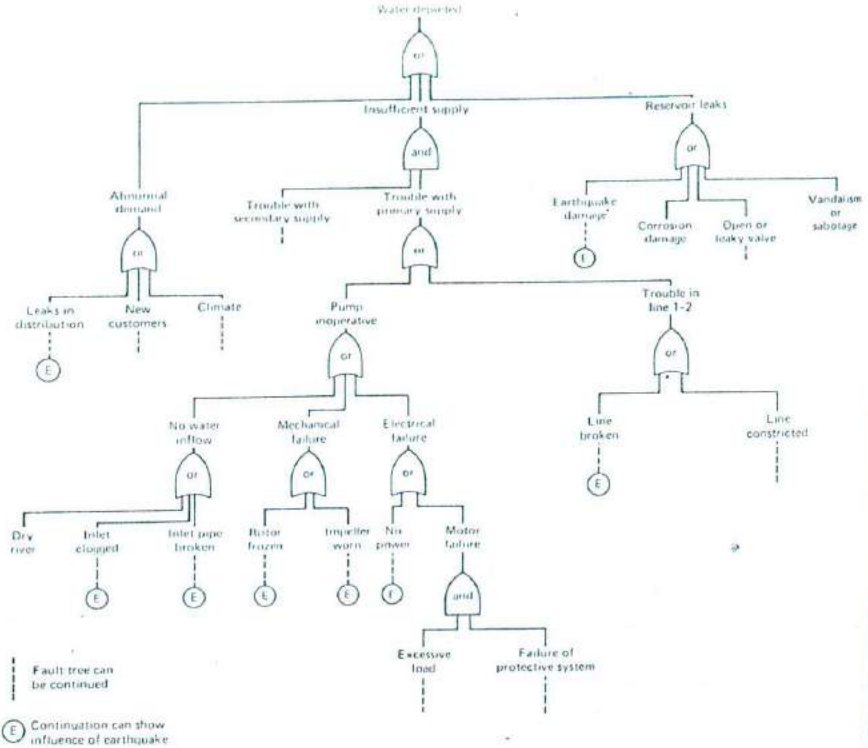


FIGURE 4-7
Fault tree for the water system shown in Fig. 4-6.

water comes out of the tap, water may still be available: from reserve tanks or from emergency delivery trucks. Thus we note that the fault-tree examination can be extended to embrace emergency measures as well.

Study Questions

1 "It is a sobering but uncertain possibility that our ability to respond to *unknown* hazards is diminished by the prevailing emphasis on control of the *known* and the specific" (Kates, 1977, *Preface*, emphasis added). Describe situations where this statement applies (for example, the past emphasis on fire hazards and the neglect of shock hazards in electrical wiring).

2 Testing is a critical step in product development and manufacture. It is not free from external influences, as the case described below reveals. Discuss how you would proceed with the testing program.

XYZ Aircraft is developing a new airplane. FAA procedures require a simulated emergency evacuation test in which the maximum number of people expected to occupy the aircraft at one time must be evacuated from it in less than 5 minutes. The test is conducted on a prototype plane in a dark hangar. It will be very expensive (insurance costs alone are considerable), and it has attracted a great deal of attention from the FAA, airline clients, and the media. The problem is that the emergency door and inflatable slide system have already revealed some serious design problems. Attempts to solve those problems have also already caused the development budget to be exceeded. Only 2 months remain until the schedule date of the test. If the plane fails it, XYZ will be greatly embarrassed, the FAA will be alerted to the problems, and an even larger financial burden will be placed on XYZ, what with the need to rerun the tests on top of the necessity still to solve the design problems themselves.

The possible actions that XYZ can take include the following:

a Expect the test to be successful. Construction of the test aircraft can proceed while design changes are made on the emergency systems. The financial savings will be great if the plane passes the test.

b Postpone the test. Allow more time for redesign. Avoid a possible rerun of the test at a high cost.

3 Draw a fault-tree diagram for the event "automobile passenger falls out of a car during accident."

4 This is a problem which involves some manipulation of logic operations and probabilistic data. It is introduced here to demonstrate that common-cause events can drastically reduce a system's (a brake's) calculated reliability.

Examine first the fault tree shown in Fig. 4-8*a*. Let P_J be the probability that event J occurs; let $\bar{P}_J$ be the probability that event J does not occur, with $\bar{P}_J = 1 - P_J$. For simplicity, let $P_D = P_E = P_F = P_G = 10^{-6}$. Then $P_B = 1 - \bar{P}_D\bar{P}_E = P_D + P_E - P_D P_E \ni 2 \cdot 10^{-6}$. Similarly $P_C \ni 2 \cdot 10^{-6}$. *The top event A* will then occur with probability $P_A = P_B P_C = 4 \cdot 10^{-12}$.

Now assume that the failure of the plunger in the rear half of the cylinder is not independent of the failure of the plunger in the front half. For instance, both failures could have originated from a mismatch in the properties of the plunger rubber and the brake fluid, thereby weakening the rubber. If such is the case, a different fault tree needs to be drawn, as shown in Fig. 4-8*b*. What is the value of P_A now?

5 List major failures of a particular type of structure. Describe the failures and discuss probable causes (faulty design, materials, construction, maintenance) and frequency of occurrence. You may consult earlier case studies and study questions and the following entries in the Bibliography. General: S. Ross (1984). b) Buildings: Hayward (1981); Klein et al (1982); McKaig (1962); McQuade (1979); Ransom (1981). c) Bridges: Fisher (1984); Kardos (1969); Petroski (1985). d) Dams: Jansen (1980). e) Airframes, ships, rails, etc.: Consult current periodical indexes.

RISK-BENEFIT ANALYSES AND INDUCEMENTS TO REDUCE RISK

Many large projects, especially public works, are justified on the basis of a risk-benefit analysis. The questions answered by such a study are the following: Is the product worth the risks connected with its use? What are the benefits? Do they outweigh the risks? We are willing to take on certain levels of

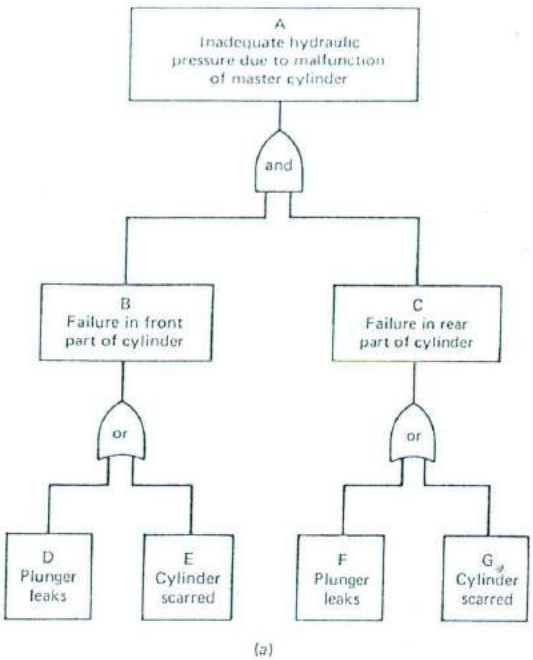


FIGURE 4-8
(*a*) Fault tree for a master brake cylinder of an automobile. (*b*) Fault tree redrawn to account for a common-mode failure. (*Adapted from Hammer, 1980, pp. 220–221.*)

risk as long as the project (the product, the system, or the activity that is risky) promises sufficient benefit or gain. If risk and benefit can both be readily expressed in a common set of units (say, dollars), it is relatively easy to carry out a risk-benefit analysis and to determine whether or not we can expect to come out on the benefit side. For example, an inoculation program may produce some deaths, but it is worth the risk if many more lives are saved by suppressing an imminent epidemic.

A closer examination of risk-benefit analyses will reveal some conceptual difficulties. Both risks and benefits lie in the future. Since there is some uncertainty associated with them, we should deal with their expected values; in other words, we should multiply the magnitude of the potential loss by the probability of its occurrence, and similarly with the gain. But who establishes these values, and how? If the benefits are about to be realized in the near future but the risks are far off (or vice versa), how is the future to be discounted in terms of, say, an interest rate so we can compare present values? What if the benefits accrue to one party and the risks are incurred by another party?

The matter of delayed effects presents particular difficulties when an analysis is carried out during a period of high interest rates. Under such circumstances the future is discounted too heavily because the very low present values of cost or benefit do not give a true picture of what a future generation will face.

How should one proceed when risks or benefits are composites of ingredients which cannot be added in a common set of units, as for instance in assessing effects on health plus aesthetics plus reliability? At most one can compare designs that satisfy some constraints in the form of "dollars not to exceed X, health not to drop below Y" and attempt to compare aesthetic values with those constraints. Or when the risks can be expressed and measured in one set of units (say, deaths on the highway) and benefits in another (speed of travel), we can employ the ratio of risks to benefits for different designs when comparing the designs.

It should be noted that risk-benefit analysis, like cost-benefit analysis, is concerned with the advisability of undertaking a project. When we judge the relative merits of different designs, however, we move away from this concern. Instead we are dealing with something similar to cost-effectiveness analysis, which asks what design has the greater merit given that the project is actually to be carried out. Sometimes the shift from one type of consideration to the other is so subtle that it passes unnoticed. Nevertheless, engineers should be aware of the differences so that they do not unknowingly carry the assumptions behind one kind of concern into their deliberations over the other.

These difficulties notwithstanding, there is a need in today's technological society for some commonly agreed upon process—or at least a process open to scrutiny and open to modification as needed—for judging the acceptability of potentially risky projects. What we must keep in mind is the following eth-

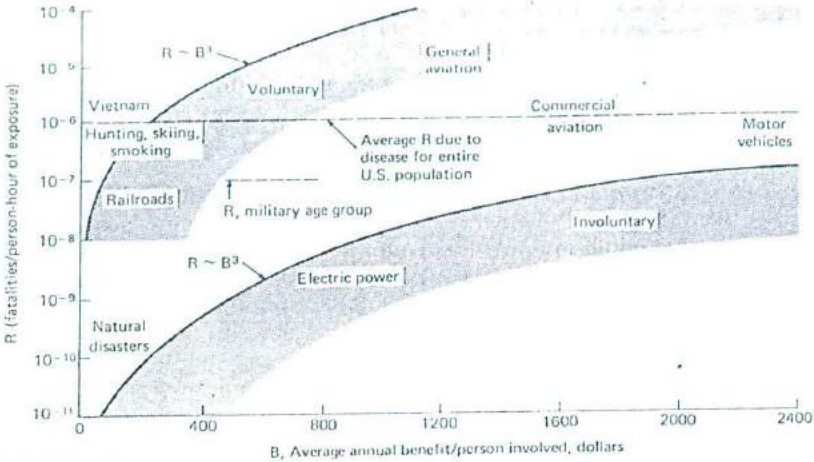


FIGURE 4-9
Willingness to assume voluntary risks as opposed to involuntary ones correlated to benefits those risks produce. (*After Starr, 1969, p. 1234.*)

ical question: *"Under what conditions, if any, is someone in society entitled to impose a risk on someone else on behalf of a supposed benefit to yet others?"* (Council for Science and Society, 1977, 37). In examining this problem further, we can trace our steps back to an observation on risk perception made earlier: A risk to a known person (or to identifiable individuals) is perceived differently by people than statistical risks merely read or heard about. Engineers do not affect just an amorphous public—their decisions have a direct impact on people who feel the impact acutely, and that fact should be taken into account equally as seriously as studies of statistical risk.

Personal Risk

Given sufficient information, an individual is able to decide whether or not to participate in (or consent to be exposed to) a risky activity (an experiment). Chauncey Starr has prepared some widely used figures which indicate that individuals are more ready to assume voluntary risks than they are to be subjected to involuntary risks (or activities over which they have no control), even when the voluntary risks are 1000 times more likely to produce a fatality than the involuntary ones. We show this graphically in Fig. 4-9.

The difficulty in assessing personal risks arises when we consider those that are involuntary. Take John and Ann Smith and their discomfort over living near a refinery. Assume the general public was all in favor of building a

new refinery at that location, and assume the Smiths already lived in the area. Would they and others in their situation have been justified in trying to veto its construction? Would they have been entitled to compensation if the plant was built over their objections anyway? If so, how much compensation would have been adequate? These questions arise in numerous instances. Nuclear power plant siting is another example. Indeed, Fig. 4-9 was produced in the context of nuclear safety studies.

The problem of quantification alone raises innumerable problems in assessing personal safety and risk, as was alluded to earlier. How, for instance, is one to assess the dollar value of an individual's life? This question is as difficult as deciding whose life is worth saving, should such choice ever have to be made.

Some would advocate that the marketplace should decide, assuming market values can come into play. But today there is no over-the-counter trade in lives. Nor are even more mundane gains and losses easily priced. If the market is being manipulated, or if there is a wide difference between "product" cost and sales price, it matters under what conditions the buying or selling takes place. For example, if one buys a loaf of bread, it can matter whether it is just one additional daily loaf among others one buys regularly or whether it is the first loaf available in weeks. Or if you are compensated for a risk by an amount based on the exposure tolerance of the "average" person, yet your tolerance of a condition or your propensity to be harmed is much greater than average, the compensation is apt to be inadequate.

The result of these difficulties in assessing personal risk is that analysts employ whatever quantitative measures are ready at hand. In regard to voluntary activities one could possibly make judgments on the basis of the amount of life insurance taken out by an individual. Is that individual going to offer the same amount to a kidnapper to be freed? Or is there likely to be a difference between future events (requiring insurance) and present events (demand for ransom)? In assessing a hazardous job one might look at the increased wages a worker demands to carry out the task. Faced with the wide range of variables possible in such assessments, one can only suggest that an open procedure, overseen by trained arbiters, be employed in each case as it arises. On the other hand, for people taken in a population-at-large context, it is much easier to use statistical averages without giving offense to anyone in particular. The ethical implications of that practice will be addressed in the following subsections. Other aspects were discussed earlier in the context of giving valid consent to participation in an experiment (see Chap. 3, under "Engineering as Experimentation").

Public Risk and Public Acceptance

Risks and benefits to the public at large are more easily determined because individual differences tend to even out as larger numbers of people are considered. The contrast between costs of a disability viewed from the stand-

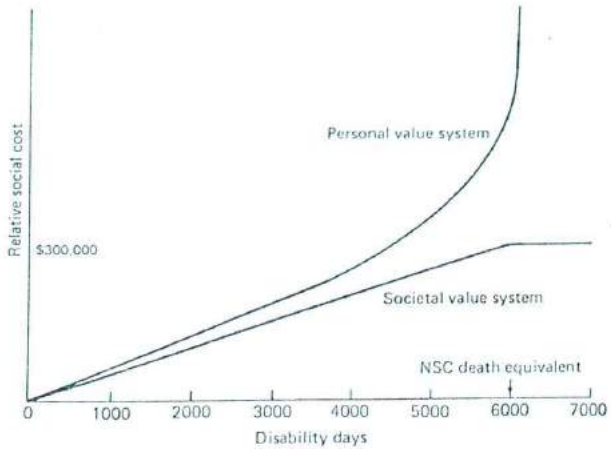


FIGURE 4-10
Value systems for social costs of disability. Using the National Safety Council equivalent of 6000 disability days for death and L. A. Sagan's 1972 assumed rate of $50 per day of disability (Sagan, 488) yields a "death equivalent" of $300,000—valid for societal value analysis only. *(After Starr, Rundman, and Whipple, 1976, p. 637.)*

point of a private value system and from that of a societal value system, for example, is vividly illustrated in Fig. 4-10. Also, assessment studies relating to technological safety can be conducted more readily in the detached manner of a macroscopic view as statistical parameters take on greater significance. In that context, the National Highway Traffic Safety Administration (NHTSA) has proposed a value for human life based on loss of future income and other costs associated with an accident. Intended for study purposes only, NHTSA's "blue-book value" amounted to $200,725 in 1972 dollars. This is certainly a more convenient measure than sorting out the latest figures from court cases. (On April 23, 1981, for example, the *Los Angeles Times* reported settlements for relatives of victims of a 1979 DC-10 crash in Chicago at $2,287,257 for a 36-year-old promising executive, $750,000 for a telephone company employee, and $275,000 for a stewardess on duty.)

A recent study by Shulamit Kahn gives a labor market value of life in the amount of $8 million. This does not include the value people place on other persons' lives, which would be 115 to 230 percent higher. "Yet even the $8 million figure is higher than is typically used in policy analysis. The unavoidable implication . . . is therefore that policy analysts do not evaluate the risk of their subjects' lives as highly as people evaluate risks to their own (and others') lives. Consequently, too many risks are taken" (Kahn, 1986).

NHTSA, incidentally, emphasized that "placing a value on a human life can be nothing more than a play with figures. We have provided an estimate

of some of the quantifiable losses in social welfare resulting from a fatality and can only hope that this estimate is not construed as some type of basis for determining the 'optimal' (or even worse, the 'maximum') amount of expenditure to be allocated to saving lives" (O'Neill and Kelley, 1975, 30).

Accounting Publicly for Benefits and Risks

The conclusions of risk assessment and cost-benefit studies are increasingly being challenged by special interest groups. And though engineers are generally reluctant to face the rough and tumble of the political and legal arenas, they are often called upon as expert witnesses in such cases. When testifying, they will find that they are treated with far more respect than perhaps equally well versed lay people who, as interested citizens, have volunteered their time to study a crucial issue. But if formal expertise bestows a certain power on engineers, it behooves them not to abuse that power. There is a noblesse oblige which demands that they remain as objective as humanly possible in their investigations and the conclusions they reach and that, in order to place their testimony in the proper perspective, they state at the outset any personal biases they may have about the subject at issue.

No expert—or even group of experts—can be expected to be omniscient. Hence the public processes designed to establish safeguards and reasonable regulations in relation to technology themselves suffer from the already mentioned problem of incomplete knowledge that engineering is subject to. Moreover, in the view of a judge who has heard many cases involving new technologies and who has written searchingly on the subject, there is yet another problem affecting public accountability for risk:

> The other kind of uncertainty that infects risk regulation comes from a *refusal to face the hard questions created by lack of knowledge*. It is uncertainty produced by scientists and regulators who assure the public that there are no risks, but know that the answers are not at hand. Perhaps more important, it is a false sense of security because the hard questions have never been asked in the first place.
>
> In the early days of nuclear plant licensing, for example, the problem of long-term waste disposal was never even an issue. Only after extensive prodding by environmental and citizens' groups did the industry and regulators show any awareness of waste disposal as a problem at all. Judges like myself became troubled when those charged with ensuring nuclear safety refused even to recognize the seriousness of the waste disposal issue, much less to propose a solution (Bazelon, 1979, 279, emphasis added).

A willingness to admit uncertainty and bias and to reveal methodology and sources is particularly important when numerical data and statistics are presented. Special caution is required when stating probabilities of rare events. We have already mentioned how conceptions of risk can vary—even be turned around—depending on how the facts are presented. How presentations of data interpretation (even the best intended) can be misleading is pointed out by W. Hammer in his discussion of the tabular material we give

TABLE 4-1
INDIVIDUAL RISK OF ACUTE FATALITY BY VARIOUS CAUSES*

Accident type	Total number for 1969	Approximate individual risk of acute fatality, probability/yr.†
Motor vehicle	55,791	3×10^{-4}
Falls	17,827	9×10^{-5}
Fires and hot substance	7,451	4×10^{-5}
Drowning	6,181	3×10^{-5}
Poison	4,516	2×10^{-5}
Firearms	2,309	1×10^{-5}
Machinery (1968)	2,054	1×10^{-5}
Water transport	1,743	9×10^{-6}
Air travel	1,778	9×10^{-6}
Falling objects	1,271	6×10^{-6}
Electrocution	1,148	6×10^{-6}
Railway	884	4×10^{-6}
Lightning	160	5×10^{-7}
Tornadoes	91	4×10^{-7}
Hurricanes	93	4×10^{-7}
All others	8,695	4×10^{-5}
All accidents		6×10^{-4}

*Use Figures with caution. See text.
†Based on total U.S. population.
Source: Rasmussen, p. 230.

here in Table 4-1. The table presents statistics on accident fatalities for the U.S. population. The approximate individual risk entries were calculated as part of a study for the U.S. Atomic Energy Commission in 1974 (Rasmussen). Hammer writes:

> The values [in Table 4-1] illustrate one problem with the use of quantitative assessments. All the fatality risk values shown are based on total U.S. population in 1969, which may not be valid in some cases. For example, if half the people of the United States do not travel by air, the probability of any one of them being killed (or of having been killed in 1969) in a plane crash is zero. The probability of the average air traveler being killed is increased to 1.8 times 10^{-5}. The probability of a person who travels more than the average (which isn't specified) is even higher. This method of risk assessment becomes even more invalid when the operation considered is one in which few persons participate. Assume that there are 160 persons killed in hang-gliding accidents in a year (the same as...[the number] killed by lightning). When the total U.S. population is used as the base for determining the risk, the probability of a fatality is 5 times 10^{-7}, as shown; a relatively safe operation. However, if there are only 20,000 enthusiasts who participate in hang gliding and they suffer a 160-person loss each year, the fatality risk is 8 times 10^{-3}. To make correct and comparable risk assessments it is therefore necessary to base them on correct and acceptable assumptions and data (Hammer, 1980, 246).

A particularly controversial study was performed by Inhaber for the Atomic Energy Control Board of Canada (Inhaber, 1979, 1982). He claimed that nonconventional energy sources, such as methanol and solar, were riskier in terms of deaths and disabling injuries (measured in workdays lost) than nuclear energy. The questions raised by the study's critics concern the lack of differentiation between injuries, the reliability of downtime data, and in connection with the latter, the casualties ascribable to replacement sources such as coal. The use of historical data (for instance, on heavy coal mine losses) and projected data (on atomic energy) also creates difficulty if one considers that coal mine safety is improving while nuclear plant safety has gone down with the bigger plants. Inhaber's report and the objections to it will make one appreciate the difficulty of preparing an objective study. (Many of the objections are quoted and rebutted in his 1982 book; other objections were raised by Shrader-Frechette, 1986). It appears that as many questions are left unanswered as are answered and the observer must conclude that decisions are made on sociopolitical grounds after all. Engineers can provide background material to support or rebut various positions, but unless they are willing to enter the debate, their contributions to the final outcome may be small. Engineers and scientists who find themselves in such situations might prefer the model of a science court, but its time has not yet arrived.

Engineers are usually asked for numbers when assessing safety and risk; therefore they should insist on meaningful numbers. This means that they should regard statistics with caution, whatever source may have issued them. Engineers should also recognize the previously mentioned difficulties with measuring risks and benefits on a cardinal scale (that is, in absolute terms), and should instead employ ordinal rankings. One of the difficulties with risk-benefit and cost-benefit analyses, again, is the matter of who does the assessing. The parties that will be affected by a project are rarely polled, especially when they are not represented by an influential lobby or trade organization (Nelson and Peterson, 1981, 2).

But difficulties in publicly accounting for risks and benefits are not related only to methods of quantification. There is also the question of justice, which involves *qualitative* value judgments:

> There are things which are wrong to do regardless of the benefits of the consequences. This is contrary to the basic assumptions in cost-benefit analysis. Without going so far as to say that consequences are never important, we can say that they are not as important as the [analyses] would imply.... The type of action one does should be morally evaluated regardless of its consequences; if it is wrong to violate certain rights, then figuring out the benefits of the consequences of doing so is irrelevant (Nelson and Peterson, 1981, 4).

Paying compensation, for example, may be an efficient and bureaucratically pleasing method for trying to make restitution when harm has been done, and indeed it is an improvement over earlier government and business procedures. But efficiency in itself does not promote ethics, as much as one

may be tempted to equate the two. As an example we may cite the attempts of the city of San Francisco in the 1960s to demolish in one fell swoop a large area slated for urban renewal. Even if the residents being displaced could have afforded to live in the new housing units once built, they would have scattered and the neighborhood would have been destroyed by the time the new dwellings were completed. The response by those residents was a near revolt which caused the city to rethink its cost-benefit formula and to set about rebuilding the area on a block by block basis, with accommodations for the temporarily displaced being provided by the city. A more expensive solution, certainly, but also more humane. And engineers need to be sensitive to such considerations.

Incentives to Reduce Risk

The engineer is faced with the formidable tasks of designing and manufacturing safe products, of giving a fair accounting of benefits and risks in regard to those products, and of meeting production schedules and helping his or her company maintain profits all at the same time. Of these objectives, product safety should command top priority. Yet this is not often so in practice, partly because of some commonly held misconceptions which militate against application of the extra thought and effort required to make a product safe.

Among the popular though faulty assumptions about safety are the following (adapted from Hammer, 1980, 52).

Assumption: Operator error and negligence are the principal causes of all accidents.

Reality: Accidents are caused by dangerous conditions that can be corrected.

For example, introduction of automatic couplers drastically reduced the number of deaths and injuries suffered by train workers. Dangerous design characteristics of products cause more accidents than failures (by fatigue, etc.) of components.

Assumption: Making a product safe invariably increases costs.

Reality: Initial costs need not be higher if safety is built into a product from the beginning. It is design changes at a later date that are costly. Even then life-cycle costs can be lower for the redesigned, safe product.

Assumption: We learn about safety after a product has been completed and tested.

Reality: If safety is not built into the original design, people can be hurt during the testing stage.

Reluctance to change a design may mean safety features will not be incorporated into the product.

Assumption: Warnings about hazards are adequate; insurance coverage is cheaper than planning for safety.

Reality: A warning merely indicates that a hazard is known to exist, and thus provides only minimal protection against harm. Insurance rates are skyrocketing. Recall actions can add to costs, even when no accidents have occurred.

Engineers should recognize that reducing risk is not an impossible task, even under financial and time constraints. All it takes in many cases is a different perspective on the design problem: a recognition from the outset that one is embarking on an experiment in which safety is an important factor.

Some Examples of Improved Safety

This is not a book on design; therefore only a few simple examples will be given to show that safety need not rest on elaborate contingency features.

The first example is the magnetic door catch introduced on refrigerators to prevent death by asphyxiation of children accidentally trapped in them. The new catch permits the door to be opened from the inside without major effort. It also happens to be cheaper than the older types of latches.

The second example is the dead-man handle used by the engineer (engine driver) to control a train's speed. The train is powered only as long as some pressure is exerted on the handle. If the engineer becomes incapacitated and lets go of the handle, the train stops automatically. Perhaps cruise controls for newer model automobiles should come equipped with a similar feature.

Railroads provide the third example as well. Old-fashioned semaphores actuated by cable usually indicated STOP when the arm was lowered. This was the position the arm assumed all by itself if the cable snapped accidentally. Here we have an early instance of a fail-safe design dating back more than a hundred years.

The motor-reversing system shown diagrammatically in Fig. 4-11 gives still another example of a situation in which the introduction of a safety feature involves merely the proper arrangement of functions at no additional expense. As the mechanism is designed in Fig. 4-11*a*, sticky contacts could cause battery B to be shorted, thus making it unavailable for further use even after the contacts are coaxed loose. A simple reconnection of wires as shown in Fig. 4-11*b* removes that problem altogether.

As a final example we mention the Volkswagen safety belt. A simple attachment on the door ensures that the belt automatically goes into place whenever one enters the car. Forgetting to strap oneself in is no longer a problem.

In the rush to bring a product onto the market, safety considerations are frequently slighted. This would not be so much the case if the venture were regarded as an experiment—an experiment which is about to enter its active phase as the product comes into the hands of the user. Space flights were carried out with such an attitude, but everyday ventures involve less obvious dangers and therefore less attention is usually paid to safety. If moral concerns alone do not sway engineers and their employers to be more heedful of

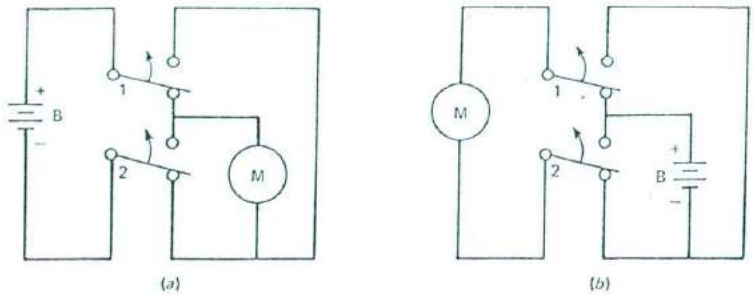


FIGURE 4-11
Motor-reversing system. (*a*) Arms 1 and 2 of the switch are both raised by a solenoid (not shown). If either one does not move—say, a contact sticks—while the other does, there is a short across the battery. The battery will discharge and be useless even after the trouble is detected. (*b*) By exchanging the positions of battery and motor, a stuck switch will cause no harm to the battery. (The motor can be shorted without harm.)

potential risks, then recent trends in product liability law should certainly do so.

Liability

The last two decades have seen a drastic change in legal protection for the consumer. Richard C. Vaughn, in his informative book *Legal Aspects of Engineering*, describes the changes as follows:

> Early English social and legal philosophy reflected the manufacturing nature of the economy. Producers of goods and services were held in high esteem. Their success meant success of the nation. The legal climate fostered their growth. Both logic and social philosophy supported the legal defense available if someone complained about a product—*caveat emptor* (the buyer beware). The logic was simple: one should examine what he is to receive before he buys it. If he is so negligent that he does not examine before he buys, then he should live with his bad bargain. Legal support of an action to recover for a bad product would be, in effect, support of buyer negligence and the law usually will not aid those who are negligent. But then, of course, the products produced in those days were somewhat more easily examined than what we buy today....
>
> Another defense in the producers' armament was "privity of contract"—the idea that one who is not a party of a contract should have no rights arising from it. In other words, if one was injured by a product but he did not buy it directly from the manufacturer, he could not act against that manufacturer to recover for his injury. The producer or manufacturer only needed to interpose a middleman—a wholesaler or retailer—as an insulator. Then, if the injured person could prove he was the buyer of the product, he might sue the middleman, but he could not reach "the deep pocket" (Vaughn, 1977, 41).

A turning point in the reversal of these attitudes came in 1916 when Judge Cordoza found the Buick Motor Company responsible for the injuries suffered by one McPherson when a wheel on a new Buick collapsed. Gradually thereafter, over a period of half a century, the notion took hold that a manufacturer can be held liable for injuries resulting from negligence in a product's design or manufacture. Still, such negligence had to be proven. Then, in 1963, the concept of strict liability was established in California by the case Greenman vs. Yuba Power Products, a concept soon thereafter incorporated into tort law by most states. *Strict liability* means it is sufficient for a product to have been defective as sold for the manufacturer to be held liable for any harm that results to users. Negligence is not at issue. What matters is that the product has a defect not obvious to users.

Despite the responsibilities implied by the doctrine of strict liability, negligence certainly remains a more grievous offense, as does breach of warranty. The latter is interpreted as a breach of contract and usually covers only the purchaser and members of the purchaser's household, not just any user. The warranty is established by advertising, labels, and other information that causes the buyer to expect a serviceable and safe product.

Engineers—and students of engineering—need to be aware of strict liability. As Richard Moll writes: "The fact that proof of negligence is not essential to impose liability is a frightening prospect for most manufacturers.... The significance of the strict liability doctrine, as far as engineers are concerned, is that although in many cases it is impossible to test every product, the engineer must weigh the chances of a defect causing serious injury against the cost of eliminating or minimizing defects in the product" (Moll, 1976, 331). Adhering to accepted practices and observing standards is not sufficient. We have labeled such behavior *minimal compliance*. It neither guarantees a safe product nor provides a valid excuse in court. As Seiden impresses on managers of engineering firms, "[standards] are excellent starting points...and they are excellent as checklists. But they must be used creatively and judgementally. They must be only the beginning, not the end, of the design process" (Seiden, 1984, 195).

While most engineers strive to be responsible in their work and have the safety of the public in mind, conditions imposed by employers may circumscribe these professional goals. On the other hand, engineers can also be sued individually, even when acting according to guidelines set by their employers. This may happen when an injured party is frustrated by laws which shield the employer or limit the employer's liability, as is the case with government agencies (the U.S. government is not liable for nuclear test fall-out). Thus it happened that one county highway engineer was sued for damages exceeding $2 million. As Dean M. Dilley reports, "The plaintiff suffered permanent injuries in an automobile accident caused by a washed out section of highway, and the suit argued that the engineer's failure to repair the road gave rise to an action for negligence against him personally" (Dilley, 1979, 12).

Some companies and government agencies protect their engineers by al-

lowing themselves to be sued for money damages over harm arising from activities of employees working within the scope of their professional duties. Engineers not so protected can resort to malpractice insurance. Independent engineers who contract for their work can minimize the effects of adverse legal judgments by writing liability limits into their contracts. This, in turn, can reduce their malpractice insurance rates. As has been mentioned before, engineering practice should be preventive or defensive in approach. A knowledge of liability is therefore well advised. Good introductory material is offered in books by Richard C. Vaughn (already mentioned) and by James F. Thorpe and William H. Middendorf (see the Bibliography).

On a larger scale, liability limitation was offered to electric utilities through the Price-Anderson Act in order to entice them into nuclear power ventures during the Atoms for Peace Program of the Eisenhower years. The $400 million limit seemed inadequate even then (it is to be raised to $7 billion), but it was probably assumed that the government would step in with disaster aid in case of a serious accident. Unfortunately the expectation of bailouts with such aid has often resulted in inadequate planning by public agencies for potential disasters of many different types, from floods to droughts, from earthquakes to conflagrations. While the Three Mile Island nuclear power plant incident of 1979 did not constitute a disaster in the usual sense, it serves as an example of the need to take safety seriously in large-scale engineering design, so it will be discussed in greater detail in the next section.

Study Questions

1 A 250,000-ton tanker (capable of holding 200,000 tons of oil) is cruising at 16 knots when engine power (25,000 hp) is lost. Control over the rudder is lost as well.
   a Estimate how long it will take in time and distance before the ship comes to a stop. Assume it had been on a straight course before the mishap. (Under normal circumstances, with reversing power available, it will take 3 miles or 22 minutes.)
   b What might be the consequences of the tanker running aground or colliding with another vessel?
   c How many tankers were lost at sea during the last decade? You may consult an almanac.
   d What are the benefits of operating a supertanker? Some are larger than 500,000 tons. Some 1-million-ton tankers have been planned. (An interesting source on this topic is Noel Mostert's book *Supership*.)
2 The following appeared in the July 10, 1981, issue of *Science*:

> The Supreme Court, in the cotton dust decision on 17 June, says explicitly that OSHA must ignore the results of any cost-benefit comparison when setting a standard for worker exposure to a hazardous substance. Justice William Brennan, writing for the court's five-person majority, said that "Congress *itself* decided the basic relationship between costs and benefits by placing the 'benefit' of the worker's health above all other considerations" when it wrote the law in 1970. Yet the agency cannot require exposure controls that are impossible to

achieve, nor can it bankrupt an entire industry, Brennan wrote. He concluded that consideration of anything besides these questions would be inconsistent with Congress's direction (R. J. Smith, 1981, 185).

Discuss this opinion of the court and how you think it might affect efforts to combat byssinosis (brown lung disease suffered by textile workers). What interpretations do you think OSHA, the textile industry, and the textile workers' unions would give this court decision? If you were an engineer in a textile plant, how would you react? Discuss your reactions in terms of their ethical foundations.

3 The following excerpt is from an article by T. W. Lockhart, "Safety Engineering and the Value of Life." Attempt to answer the question posed by Lockhart. Try again after you have finished reading this entire chapter.

> ...there is an honored tradition in moral philosophy, associated primarily with Immanuel Kant, according to which human beings have a worth that is not commensurable with that of mere objects. According to this view, because of this incommensurability we must recognize and respect the liberty and dignity of each person and refrain from treating him merely as a means to some end. Human beings may not be used in order to achieve some higher good, for there is no higher good. Let us call this view the Incommensurability Principle.
>
> The Incommensurability Principle has had a powerful appeal for many. This has been true mainly because it has been felt that unless it, or something like it, is accepted it is not possible to account for such fundamental human rights as the right not to be killed, the right not to have one's liberty abridged without just cause, and the right to be treated fairly and honestly. The Incommensurability Principle is clearly incompatible with an attempt to place a monetary value on human life or to justify actions on the basis of such a valuation. There is thus further reason for doubting the wisdom of any such attempt....
>
> Is it possible to reconcile the Incommmensurability Principle with the commonsense view that considerations of safety must be weighed against economic costs? (Lockhart, 1981, 3)

4 During the early stages of its development, crashworthiness tests revealed that the Pinto, a Ford automobile, could not sustain a front-end collision without the windshield breaking. A quick-fix solution was adopted: The drive train was moved backward. As a result the differential was moved very close to the gas tank (Camps, 1981, 119-129). Thus many gas tanks collapsed and exploded upon rear-end collisions once the Pinto became available to the public. Extensive lawsuits followed (Strobel, 1980; Cullen, 1987). Study the Pinto story and write it up as a case study. You may use the Predicasts F&S (Funk and Scott) Index of Corporations and Industries (Predicasts, Inc., Cleveland, Ohio) to find additional references.

5 The U.S. Consumer Product Safety Commission states the following in its 1981 annual report:

> Each year, an estimated 36 million Americans are injured and 30,000 are killed in accidents involving consumer products. The cost of these accidents is staggering—over $12.5 billion annually in medical costs and lost earnings.

These figures have been repeatedly cited in the literature to impress on engineers

the need to design safe products. Review the data presented by the Commission in its annual and monthly reports and estimate what portion of the figures can be rightfully ascribed to poor design and what portion to consumer carelessness.

6 Only about 15 years ago 600 women reportedly lost hands (one, not both, we hope) in top-loading washing machines every year (Papanek, 75). If you had been in the business of manufacturing washing machines then, how do you think you might have reacted and should have reacted to such statistics?

7 A worker accepts a dangerous job after being offered an annual bonus of $2000. The probability that the worker may be killed in any one year is 1/10,000. This is known to the worker. The bonus may therefore be interpreted as a self-assessment of life with a value equal to $2000 divided by 1/10,000, or $20 million. Is the worker more or less likely to accept the job if presented with the statistically identical figures of a $100,000 bonus over 50 years (neglecting interest) and a 1/200 probability of a fatal accident during that period?

8 As emerging technologies have reduced risks from some sources, other risks have frequently become prominent. For instance, efforts to combat famine by drawing and transporting water for irrigation brought early benefits coupled with lasting problems to such diverse areas as Mesopotamia and the Andes in the past, or to the Punjab and the Sahel in the present. We also observe that the decrease in infectious disease was accompanied by an increase in chronic disease. Give another similar example and discuss it as a problem in risk-benefit analysis.

9 The owner of a television set brought legal action against its manufacturer (Admiral) seeking compensatory and punitive damages for severe burns and other injuries suffered when the set burst into flames. It was revealed at the trial that other sets made by the manufacturer had also gone up in smoke and flames. Prepare a case study for use in discussing the legal and ethical implications of the manufacturer's actions (or lack thereof). The case is Zora H. Gillham vs. The Admiral Corporation. It was brought to the authors' attention by Donald E. Wilson. An early report appeared in the *Federal Reporter*, 2d series, vol. 253, F.2d, West Publishing Co., St. Paul, Minnesota, 1976. Consult the current literature.

10 "Airless" paint spray guns do not need an external source of compressed air connected to the gun by a heavy hose (although they do need a cord to attach them to a power source) because they have incorporated into them a small electric motor and pump. One common design uses an induction motor which does not cause sparking since it does not require a commutator and brushes (which are sources of sparking). Nevertheless the gun carries a label, warning users that electrical devices operated in paint spray environments pose special dangers. Another type of gun which, like the first, also requires only a power cord, is designed to weigh less by using a high-speed universal motor and a disk-type pump. The universal motor *does* require a commutator and brushes, which cause sparking. This second kind of spray gun carries a warning similar to that attached to the first, but it states in addition that the gun should never be used with paints which employ highly volatile and flammable thinners such as naphtha. The instruction booklet is quite detailed in its warnings.

A painter had been lent one of the latter types of spray guns and was operating it while it was partially filled with paint thinner in order to clean it out. It caught fire, and the painter was severely burned as the fire spread. The instruction booklet pointing out the spray gun's dangers was in the cardboard box in which the gun was kept, but it had not been read by the painter, who was a recent immi-

grant and did not read English very well. Do you see any ethical problems in continuing over-the-counter sales of this second type of spray gun? What should the manufacturer of this novel, lightweight device do?

In answering these questions, consider the fact that courts have ruled that hidden design defects are not excused by mere warnings attached to the defective products or posted in salesrooms. Informed consent must rest on a more thorough understanding than can be transmitted to buyers by simple warning labels.

11 Discuss the ethical aspects of various methods of measuring benefits and costs described by Bailey (1980) and/or, Shrader-Frechette (1985, 2 books). This may take the form of book reports.

12 Industry generally maintains that restrictive regulations on potentially toxic substances should be enacted only after it has been proven by rigorous scientific methods that a link exists between health effects and a pollutant. The opposition to this viewpoint argues that "waiting for firm evidence of human health effects amounts to using the nation's people as guinea pigs, and that is morally unacceptable. It proposes that far from overestimating the risks from toxic substances, conventional risk assessments underestimate them, for there may be effects from chemicals in combination that are greater than would be expected from the sum effects of all chemicals acting independently" (Ruckelshaus, 1987, 27). What are the risk management problems when *several* pollutants from *several* sources contribute to an areawide pollution problem but are regulated by *several* different agencies, each of which "has statutory authority to regulate the use and emission of *some* of the substances from *some* of the sources, in *some* of the pathways, for the purpose of protecting *some* of the population under *some* circumstances"? (Baram, 1976)

THREE MILE ISLAND AND CHERNOBYL: THE NEED FOR SAFE EXITS

As our engineering systems grow more complex, it becomes more difficult to operate them. As Charles Perrow (see Bibliography) argues, our traditional systems tended to incorporate sufficient slack, which allowed system aberrations to be corrected in a timely manner. Nowadays, he points out, subsystems are so tightly coupled within more complex total systems that it is not possible to alter a course safely unless it can be done quickly and correctly. Frequently the supposedly corrective action taken by operators may make matters worse because they do not know what the problem is. At Three Mile Island, for instance, so many alarms had to be recorded by a printer that it fell behind by as much as 2½ hours in reporting the events.

Designers hope to ensure greater safety during emergencies by taking human operators out of the loop and mechanizing their functions. The control policy would be based on predetermined rules. This in itself creates problems because (1) not all eventualities are foreseeable, and (2) even those that can be predicted will be programmed by an error-prone human designer (Senders, 1980). In addition, another problem arises when (3) the mechanized system fails and a human operator has to replace the computer in an operation that demands many rapid decisions. The proposed air traffic con-

trol system allowing for 10-second separation between planes would fall into this category.

Operator errors were the main causes of the nuclear reactor accidents at Three Mile Island and Chernobyl. Beyond these errors a major deficiency was revealed at both installations: inadequate provisions for evacuation of nearby populations. This lack of "safe exit" is found in too many of our otherwise amazingly complex systems. After examining the reactor incidents we shall discuss this wider issue.

Three Mile Island

Walter Creitz, president of Metropolitan Edison, the power company in the Susquehanna Basin, was obviously annoyed by a series of articles in the *Record*. This local, daily newspaper of York, Pennsylvania, had cited unsafe conditions at Metropolitan Edison's Three Mile Island nuclear power plant Unit 2. Creitz dismissed the stories as "something less than a patriotic act—comparable in recklessness... to shouting 'Fire!' in a crowded theater." A few days later a minor malfunction in the plant set off a series of events which made "Three Mile Island" into household words across the world (Rogovin, 1980, 3).

Briefly, this is what happened (for details see Kemeny, 1979; Rogovin, 1980; Ford, 1982; Mason, 1979; Moss and Sills, 1981; Keisling, 1980; D. Martin, 1980). At 4 A.M. on March 28, 1979, Unit TMI-2 was operating under full automatic control at 97 percent of its rated power output. For 11 hours a maintenance crew had been working on a recurring minor problem. Resin beads are used in several demineralizers (labeled 14 in the schematic diagram shown as Fig. 4-12) to clean or "polish" the water on its way from the steam condenser (12) back to the steam generator (3). Some beads had clogged the resin pipe from a demineralizer to a tank in which the resin is regenerated. In flushing the pipe with water, perhaps a cupful of water backed up into an air line which provides air for fluffing the resin in its regeneration tank. But that air line is connected to the air system which also serves the control mechanisms of the large valves at the outlet of the demineralizers. Thus it happened that these valves closed unexpectedly.

With water flow interrupted in the secondary loop (26), all but one of the condensate booster pumps turned off. That caused the main feedwater pumps (23) and the turbine (10) to shut down as well. In turn, an automatic emergency system started up the auxiliary feedwater pumps (25). But with the turbines inoperative, there was little outlet for the heat generated by the fission process in the reactor core. The pressure in the reactor rose to over 2200 pounds per square inch, opening a pressure-relief valve (7) and signaling a SCRAM, in which control rods are lowered into the reactor core to stop the main fission process.

The open valve succeeded in lowering the pressure, and the valve was readied to be closed. Its solenoid was deenergized and the operators were so

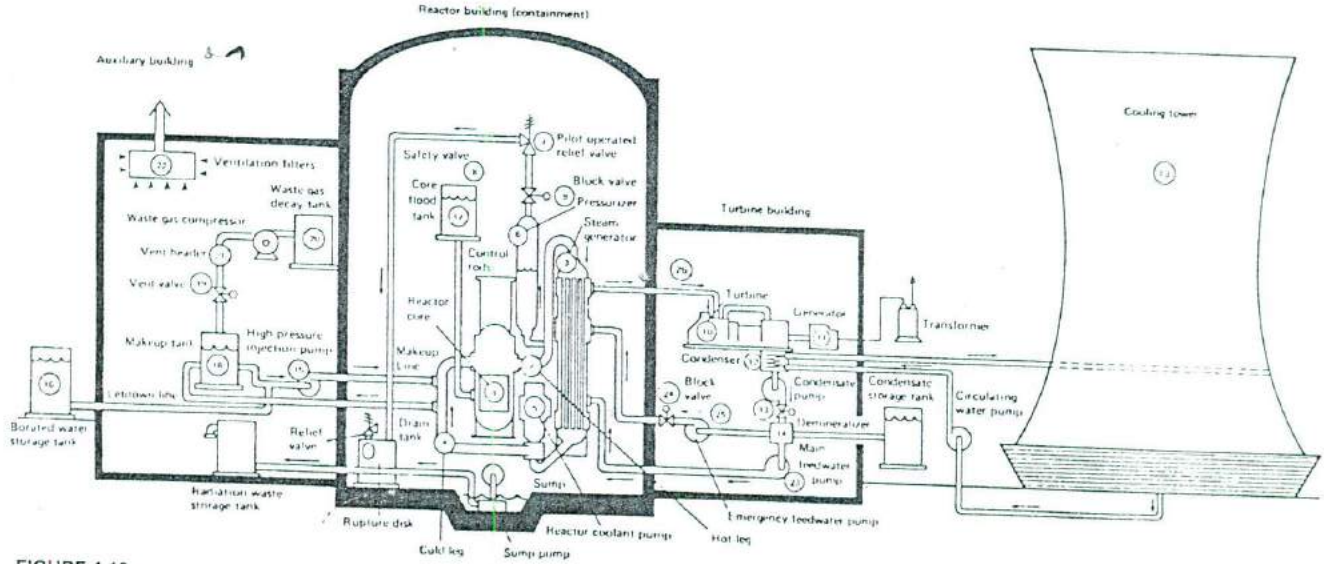


FIGURE 4-12
Schematic diagram of Three Mile Island nuclear power plant Unit 2. Pressurized water reactor system: Heat from reactor core (1) is carried away by water in a primary loop (1, 2, 3, 5, 4). In steam generator (3) the heat is transferred to water in a secondary loop (26) at lower pressure. The secondary-loop water turns to steam in the steam generator or boiler (3), drives the turbine (10), turns into water in the condenser (12), and is circulated back to (3) by means of pumps (13, and 23 and 25). (*Adapted from* IEEE Spectrum, *November 1979, copyright ©1979 by the Institute of Electrical and Electronics Engineers, Inc., and from Rogovin and Frampton, 1980.*)

informed by their control-panel lights. But something went wrong: The valve remained open, contrary to what the control panel indicated. Apart from this failure everything else had proceeded automatically as it was supposed to. Everything, that is, except for one other serious omission: The pumps (25) could not supply the auxiliary feed water because block valves 24 had inadvertently been left closed after maintenance work done on them two days earlier. Without feedwater in loop 26 the steam generator (3) boiled dry. Now there was practically no heat removal from the reactor, except through the relief valve. Water was pouring out through it at the rate of 220 gallons per minute. The reactor had not yet cooled down, and even with the control rods shutting off the main fission reaction there would still be considerable heat produced by the continuing radioactive decay of waste products.

Loss of water in the reactor caused one of a group of pumps, positioned at 15, to start automatically; another pump was started by the operators to rapidly replenish the water supply for the reactor core. Soon thereafter the full emergency core-cooling system went into operation in response to low reactor pressure. Low reactor pressure can promote the formation of steam bubbles which reduce the effectiveness of heat transfer from the nuclear fuel to the water. There is a pressurizer which is designed to keep the reactor water under pressure. (The relief valve sits atop this pressurizer.) The fluid level in the pressurizer is also used as an indirect—and the only—means of measuring the water level in the reactor.

The steam in the reactor vessel caused the fluid level in the pressurizer to rise. The operators, thinking they had resolved the problem and that they now had too much water in the reactor, shut down the emergency core-cooling system and all but one of the emergency pumps. Then they proceeded to drain water at a rate of 160 gallons per minute from the reactor, causing the pressure to drop. At this point they were still unaware of the water escaping through the open relief valve. Actually they assumed some leakage, which occurred because of poor valve seating even under normal circumstances. It was this which made them disregard the high-temperature readings in the pipes beyond 7.

The steam bubbles in the reactor water covered much of the fuel, and the tops of the fuel rods began to crumble. The chemical reaction between the steam and zircaloy covering the fuel elements produced hydrogen, some of which was released into the containment structure, where it exploded.

The situation was beginning to get really serious when, 2 hours after the initial event, the next shift arrived for duty. With some fresh insights into the situation, the relief valve was deduced to be open. Blocking valve 9 in the relief line was then closed. Soon thereafter, with radiation levels in the containment building rising, a general alarm was sounded. While there had been telephone contact with the Nuclear Regulatory Commission (NRC), as well as with Babcock & Wilcox (B&W), who had constructed the reactor facility, no one answered at NRC's regional office and a message had to be left with

an answering service. The fire chief of nearby Middletown was to hear about the emergency on the evening news.

In the meantime, a pump was transferring the drained water from the main containment building to the adjacent auxiliary building, but not into a holding tank as intended; because of a blown rupture disk, the water landed on the floor. Eventually there was to be sufficient airborne radiation in the control room to force evacuation of all but essential personnel. Those left behind wore respirators, making communication difficult.

Eventually the operators decided to turn the high-pressure injection pumps back on again, as the automatic system had been set to do all along. The core was covered once more with water, though there were still some steam and hydrogen bubbles on the loose. Thirteen and one-half hours after the start of the episode there was finally hope of getting the reactor under control. Confusion over the actual state of affairs, however, continued for several days.

Nationwide the public watched television coverage in disbelief as responsible agencies displayed their lack of emergency preparedness at both the reactor site and evacuation-planning centers. More than 8 years later, the decommissioning of the reactor was still not complete. Its radioactive water had been decontaminated, but only one-half of the 300,000 pounds of core debris had been gingerly removed. The cleanup alone was expected to cost over a billion dollars. Three Mile Island was a financial disaster.

Prior Warnings

Apart from the technical lessons learned at the Three Mile Island "laboratory," the experience has offered lessons in the need for disaster planning and openmindedness. "Openmindedness" refers, once again, to not allowing a preoccupation with rules to prevent close examination of safety problems which may not be covered by rules. It also refers to a willingness on the part of management to take seriously the safety concerns expressed by engineers within or outside the organization. A lack of concern in this direction is particularly troubling, as exemplified by the experience of a number of engineers who reported dangerous behavior of B&W reactors of the type used at Three Mile Island well before the accident. A selection follows.

Stephen Hanauer, a government nuclear safety expert, communicated in 1969 to then Atomic Energy Commission head Glenn Seaborg his concern regarding common-mode failure possibilities at nuclear power plants. Later he became particularly worried about the poor performance record of valves in nuclear power plants. He also decried the lack of proper analysis of field reports which would help identify weak spots in design (Ford, 1982, 53-61).

As it turned out, the largest single failure at TMI *was* of a common-mode type, although not of a physical nature, as is more usual. It lay in the oper-

ators' inadequate training. No one on duty at the plant that early morning of March 28 was a nuclear engineer, and no one was even a college graduate; no one in charge was trained to handle complex reactor emergencies. [Interestingly enough, the 1974 Rasmussen Report on nuclear power plant safety (see the Bibliography) had singled out human response as the weakest link in plant reliability.]

Moreover, Hanauer's concern over valves was well founded. Problems with valves have not been restricted to the nuclear industry, and the particular type of relief valve that malfunctioned at TMI had done so earlier at other nuclear power plants. In fact, since 1970 eleven pilot-operated relief valves had stuck open at other such plants (Lombardo, 1980, 55).

2 John O'Leary, Deputy Secretary of Energy when he presided at the opening ceremonies of TMI's Unit 2, had earlier prepared a memo for incoming President Carter. Then a deputy director for licensing at the Atomic Energy Commission, he had written that "the frequency of serious and potentially catastrophic nuclear incidents supports the conclusion that sooner or later a major disaster will occur at a major generating facility" (Ford, 1982, 15). Yet the probability of serious accidents continued to be given such a low value that it was not thought necessary to plan for orderly emergency measures involving off-site populations and agencies.

3 James Creswell was a reactor inspector for the NRC assigned to the startup of Toledo Edison's Davis-Besse nuclear generating station, which also used a reactor built by B&W. Reading a B&W report on some strange behavior of its unit at Rancho Seco in California following the accidental dropping of a small light bulb into the main control panel, Creswell noticed startling similarities to an incident which had occurred at Davis-Besse during low-power tests in September 1977. A severe and sudden increase in heat had taken place in both cases, at Rancho Seco because of faulty control signals produced by difficulties with the control panel and at Davis-Besse because of failure of the main feedwater system. At both plants the instruments had not given the operators adequate indication of the reactors' true operating conditions. At Davis-Besse the pressure-relief valve had stuck open and the operator had misinterpreted the level of water in the reactor based on indications of the level in the pressurizer. This had led them to mistakenly shut off the emergency core-cooling pumps, even at Davis-Besse. The only differences were that Davis-Besse had been operating at 9 percent of rated capacity (as against 96 percent at TMI) and the failure of the relief valve to close had been detected after 22 minutes (instead of more than 2 hours as at TMI).

Creswell worried about this and, from early 1978 on, tried to communicate his concerns to various parties at the NRC, the utility, and B&W. Eventually he took a day off and flew at his own expense to Bethesda, Maryland. There he met with two NRC commissioners who were willing to listen. The result was a memo to the NRC staff requesting answers to some of Creswell's questions. The memo was delivered the day after the TMI incident.

While the similarities between what happened at Davis-Besse and at Rancho Seco are of interest, the near duplication at TMI of the occurrences at Davis-Besse makes a strong case for the free exchange of information and expeditious correction of faults, unfettered by organizational expediencies or short-range interests. And an ironic twist to the story points out clearly what approaches to safety are usually the more valued: Creswell eventually received a special NRC award of $4000 for his efforts. Two other officials, who had earlier been unresponsive to Creswell's pleas, were awarded $10,000 and $20,000 each for their efforts during the ensuing dramatic emergency at TMI (Ford, 1982, 72-82).

4 Also late in 1977, Carlyle Michelson, a senior nuclear engineer with the Tennessee Valley Authority (TVA), had been questioning safety aspects of a new B&W reactor for TVA's Bellefonte Nuclear Plant. Included in his analysis was the possible formation of a steam bubble in the reactor's cooling-water system, something which had also been mentioned by Creswell. Michelson's study, which additionally mentioned the dangers of misreading the reactor coolant level by looking at the pressurizer, received some support on its way to the NRC's Division of System Safety. If handled according to protocol, the memo should have been sent on to the Division of Operating Reactors, whence reactor users, particularly at Davis-Besse, would have been alerted to the problems. The assistant director of the Division of System Safety later said that the Davis-Besse analysis was the responsibility of the Office of Inspection and Enforcement. He thought they would have taken action if any was needed. Ten days after the TMI incident, the Advisory Committee on Reactor Safeguards asked the NRC to carry out some of Michelson's recommendations (Ford, 1982, 82-84).

5 At B&W, meanwhile, the 1977 occurrence at Davis-Besse caused concern. Before the TMI incident the company did not have any formal procedure to analyze ongoing problems at B&W-equipped plants or to study reports filed by its customers with the NRC. B&W was busy building and shipping new reactors. Nevertheless, the Davis-Besse incident was sufficiently unusual that B&W engineers were sent out to investigate. Some individuals maintained their interest and tried—in vain—to get word out to B&W customers: John Kelly, a plant-integration engineer; Bert Dunn, manager of emergency-cooling-system analysis; and Donald Hallman, a customer service employee. Internal B&W memos later revealed the company's awareness of reactor defects. The company denied NRC charges that it had failed to notify the Commission, but it instituted measures to make sure that this would not occur again (Ford, 1982, 86-92).

Chernobyl

The nuclear power plant complex at Chernobyl, near Kiev (Ukraine, U.S.S.R.) had four reactors in place by 1986. With the planned addition of Units 5 and 6, for which foundation work was underway, the site would be

the world's second largest electric power plant park, with an output of 6000 megawatts (electrical). The reactors are of a type referred to as RBMK; they are graphite-moderated and use boiling-water pressure tubes. Chernobyl and the Russian nuclear power program were prominently featured in 1985 issues of the English language periodical *Soviet Life*. The articles featured the safety of atomic energy and the low risk of accidents and radiation exposure. For readings on the accident and its aftermath we refer the reader to Hawkes et al. (1986), Marples (1986), Edwards (1987), and Ahearne (incl. disc., 1987).

On April 25, 1986, a test was underway on reactor 4 to determine how long the mechanical inertia of the turbine-generator's rotating mass could keep the generator turning and producing electric power after the steam supply was shut off. This was of interest because reactor coolant pumps and other vital electric machinery have to continue functioning though the generators may have had to be disconnected suddenly from a malfunctioning power grid. Special diesel generators will eventually start to provide emergency power for the plant, but diesel units cannot always be relied upon to come up promptly. This test was undertaken as part of a scheduled plant shutdown for general maintenance purposes.

It requires 3600 megawatts of thermal power in the reactor to produce 1200 megawatts at the generator output. Unit 4 had been gradually reduced from 3200 megawatts (thermal) to 1600 megawatts and was to be slowly taken down to between 1000 and 700 megawatts, but at 2 P.M. the power dispatch controller at Kiev requested that output be maintained to satisfy an unexpected demand. This meant a postponement of the test. In preparation for the test the reactor operators had disconnected the emergency core-cooling system so its power consumption would not affect the test results. This was to be the first of many safety violations. Another error occurred when a control device was not properly reprogrammed to maintain power at the 700- to 1000-megawatt level. When at 11:10 P.M. the plant was authorized to reduce power, its output dropped all the way to 30 megawatts, where the reactor is difficult to control. Instead of shutting down the reactor, the operators tried to keep the test going by raising the control rods to increase power. Instead of leaving fifteen controls inserted as required, the operators raised almost all control rods because at the low power level the fuel had become poisoned by a buildup of xenon-135, which absorbs neutrons.

The power output stayed steady at 200 megawatts (thermal)—still below what the test called for—but the test was continued. In accord with the test protocol, two additional circulating pumps were turned on to join the six already in operation. Under normal levels of power output this would have contributed to the safety of the reactor, but at 200 megawatts it required many manual adjustments to maintain the balance of steam and water. "The operators at this point recognized that because of the instabilities in this reactor and the way xenon poisoning builds up, once the reactor is shut down, they would have to wait a long time before starting it up again" (Ahearne,

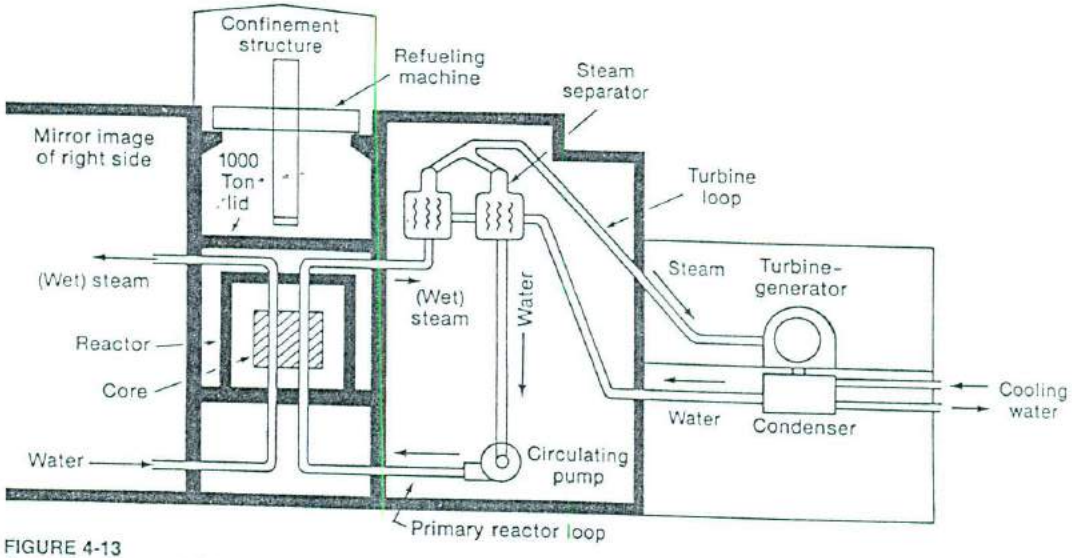


FIGURE 4-13
Schematic diagram of Reactor 4 at Chernobyl. This RBMK-type reactor produces steam for two 500-megawatt steam turbine generators, only one of which is shown. (*After Ahearne, 1987, p. 674.*)

1987). So, deciding to proceed with the test, the operators blocked the emergency signals and automatic shutdown controls because they would have gone into action upon removal of the electrical load.

"The reactor was now running free, isolated from the outside world, its control rods out, and its safety system disconnected." As Legasov, the U.S.S.R. representative to the International Atomic Energy Commission, told the conference reviewing the accident in Vienna: "The reactor was free to do as it wished" (Hawkes et al., 1986, 102).

At 1:23 A.M. the test began. When the steam valves were closed and its load was effectively removed, the reactor's power and temperature rose sharply. Unlike water-moderated reactors, the graphite-moderated RBMK reactor uses water only as a heat-transfer medium, not as a moderator. As the core becomes hotter it allows fission to increase. This positive feedback effect produced a surge of power in Chernobyl's reactor 4, from 7 percent to hundreds of times its rated thermal output. "The effect was the equivalent of ½ ton of TNT exploding in the core.... The fuel did not have time to melt... it simply shattered into fragments" (Hawkes et al., 1986). The fuel, bereft of its cladding, came in contact with the water. A second explosion occurred (very likely a steam explosion). It lifted and shifted a 1000-ton concrete floor pad separating the reactor from the refueling area above it. The zirconium cladding of the fuel rods interacted with the circulating water to form hydrogen. This produced a spectacular display of fireworks. A shower of glowing graphite and fuel spewed over the compound while a radioactive plume was driven sky high by the heat.

What followed was as inexcusable as what had caused the accident. While valiant firefighters lost their lives extinguishing the blaze, it took hours to warn the surrounding communities. Only when alert nuclear plant operators in Sweden detected an increase in radioactivity did Moscow learn that something was amiss. The Soviet republics and the rest of Europe did not know how to handle such a grave event, especially not the radioactive fallout. Many blamed Moscow for not notifying them but had no monitoring devices of their own, not even to check on their local nuclear plants. Instructions on what to do about drinking milk, eating vegetables, letting children play outside, and other concerns of the populations of Europe depended more on the political leanings and the pronuclear or antinuclear stance of the health minister issuing a directive.

Acute radiation sickness, combined with burns, severely affected about 200 Chernobyl plant workers, of whom 31 died. The 1000 families living in a workers' settlement 1 mile from the plant were evacuated 12 hours after the explosion, but the plant had no responsibility for, nor direct link with, the communities beyond a 1.5-mile radius. The evacuation of nearby Pripyat and 71 villages within 18 miles of the plant started the next day. About 120,000 people had to be moved by buses and trucks. Numerous new villages were constructed to house the displaced. The near- and long-term effects of radi-

ation on the people and fauna of Europe will be widely discussed for many years.

It took one week to contain the fire by covering the reactor with a mix of sand, clay, and dolomite deposited by helicopters. Tunnels were dug underneath the reactor to install cooling pipes carrying liquid nitrogen. The tunnels also served to lay down a concrete layer to prevent leakage of radioactive water to the aquifer. Eventually the entire plant was completely entombed in concrete.

Three Mile Island, Chernobyl, and a Hushed-up Forerunner

There are similarities and dissimilarities between the events at Three Mile Island and Chernobyl, but the lessons to be learned do not differ much.

Pressurized-water reactors (PWR) as used at TMI have strong containment structures. Thus the radioactive products of the accident at TMI Unit 2 were fairly well contained. The RBMK reactors at Chernobyl have a much weaker containment system relative to the space into which gases and steam can expand during an accident. It should be noted that many reactors in the United States also do not have a sturdy containment. Examples of such less well protected types are the ones producing weapons-grade plutonium for the U.S. Department of Energy and the earlier versions of boiling-water reactors. Such units depend on special cooling methods to limit pressure rises and to keep radioactive gases within confinement structures (which are smaller and weaker than containment structures).

Both reactor types are sensitive to perturbations. Three Mile Island's PWR has a once-through reactor-cooling system with a rather small amount of water and an undersized pressurizer. The RMBK exhibits a positive temperature-power feedback which at low power levels is not sufficiently offset by the negative fuel temperature coefficient.

Also common to both plants was the complacency shown by management and operators, largely created by the absence of prior, major accidents at their respective sites. What happened elsewhere was either "out of sight, out of mind" or greeted by "It can't happen here." This is how the engineers at Chernobyl had felt about TMI, and how more recently the Chernobyl episode was received elsewhere. But serious accidents can happen, and when they do, they usually occur in ways not foreseen—which is what makes them serious. The physical layout of systems may be different from plant to plant and country to country, but managers and operators are never so different in their behavior. At TMI, operating procedures were not continuously and thoroughly reviewed by experts. At Chernobyl, the test protocol had not even been discussed with plant designers and nuclear engineers or physicists. At neither plant were the operators fully conversant with the operating principles of the plant equipment.

Discussions regarding dangers to the public at the time of the events at

TMI and Chernobyl became "mass-mediated" events (a term used by some in connection with Bhopal), while engineers, physicists, physicians, health officials, and regulators were unable to issue authoritative status reports and offer professionally sound advice. The official reports that eventually came from the Soviet Union were refreshingly candid. In the past, moreover, secrecy had not been a monopoly of the U.S.S.R. In the United States, the former Atomic Energy Commission had kept information about embarrassing events close to its chest; so did the atomic energy establishment in the United Kingdom, where the Windscale nuclear plant had emitted so much radioactive material that its name was changed to Sellafield to deflect attention.

Not only did Windscale discharge ¼ ton of plutonium into the Irish sea and experience several leaks, it also had a reactor fire in 1957, with graphite and uranium fuel cladding ablaze for 42 hours. Efforts at extinguishing the fire with the carbon dioxide system provided for this purpose had failed. Only by gambling on extinction by a "tidal wave" of water to forestall a steam explosion during its application was the plant saved. Fortunately most of the potential radioactive fallout was trapped by special filters installed at the insistence of Sir John Cockcroft, who had worked on atomic bombs. Before the accident the filters had been jokingly called Cockcroft's Folly because they were felt to be superfluous. Even with those filters enough fallout escaped to require eventual disposal of 2 million liters of milk in a 500-square-mile area. The reactor was smaller than the Chernobyl unit and not all of it was demolished. Yet it took 10 years before dismantling could begin, and for over two decades the official reports of an inquiry were not released to the public to protect the nuclear industry.

Central Europe has the greatest concentration of atomic power in the world, with 388 plants in operation or in some phase of construction and planning. Electricité de France (EdF) is often cited as a model of nuclear plant operation. By concentrating on standardized designs early on (a gamble, because the standards could have turned out to be poor), and insisting on highly trained personnel, an excellent safety record has been accumulated (except for nuclear-fuel-reprocessing at La Hague). Yet, to the people on the other side of the Rhine the lack of joint emergency exercises involving the nuclear reactor parks across the borders in France is not reassuring.

Financially the nuclear power industry is facing a bleak picture in the United States. Not only were there high costs associated with the major accidents, but the growing cost of building the plants without error and to increasingly stringent requirements, coupled with a decline and reversal in the rate of growth of fossil fuel prices, has raised havoc with the economic side of the industry. The Washington Public Power Supply System, which had invested heavily in nuclear power plants, had to mothball two of its reactors and has a multibillion-dollar debt. Electricité de France is the world's largest debtor: $200 billion. In the meantime some incomplete nuclear plants are being converted to fossil fuel operation in the United States.

The nuclear industry and its regulators have not been open with the pub-

lic. They must have felt that the public cannot be trusted, that it is too easily swayed by "Luddites and scare mongers." In France the protests against nuclear energy have been squelched by strong police measures and secrecy. "You don't tell the frogs when you are draining the marsh," said the director of EdF (Hawkes et al., 1986, 67). Nevertheless it has been noticed by the public that regulators' figures for "safe" doses of radiation exposure have been lowered again and again over the years. (Further reductions are likely to follow in the wake of revelations that the Hiroshima casualties were produced by less radiation exposure than had been calculated hitherto). It is also no secret that insurance companies are not willing to underwrite policies covering the full potential losses incurred by an accident (which makes measurement of perceived risk by the method of examining insurance policies impossible here). Finally, residents near many nuclear plants know how inadequate emergency evacuation plans are.

The public mistrust which the nuclear industry and its regulators have earned is unfortunate because nuclear power is an alternative we must seriously consider as our fossil fuels become scarcer, rise in price once again, or become otherwise inaccessible. Much more is required in the way of candid, intelligent discourse and action if the public is to be expected to underwrite continued experiments with nuclear power. An unusual undertaking in this respect was the 1-year educational program sponsored by the Swedish government prior to a public referendum on whether or not the nuclear energy program in that country should be terminated and existing plants be phased out. Supporters and opponents were given public funds to broadcast programs in support of their positions.

Safe Exit

In our Chap. 2 discussion we based the engineer's responsibility for safety on considerations of ethics. In this chapter we have described how risks are perceived, assessed, and weighed against benefits; also how engineers ultimately are faced with designing as much safety into their products as feasible under constraints of knowledge, time, cost, and clients' wishes. We stated in Chap. 3 that the tough part of the engineering experiment begins when the product is put to use. Let us pick up the thread at that juncture.

It is almost impossible to build a completely safe product or one that will never fail. The best one can do is to assure that a product—if and when it fails—will fail safely, that the product can be abandoned safely, or that the user can safely escape the product. Let us refer to these three conditions as *safe exit*. It is not obvious who should take the responsibility for providing safe exit. But apart from questions of who will build, install, maintain, and pay for a safe exit system there remains the crucial question of who will think of the need for a safe exit.

It is our position that providing for a safe exit is an integral part of the experimental procedure—in other words, of sound engineering. The experi-

ment is to be carried out without causing bodily or financial harm. If it does, it must be terminated safely. The full responsibility cannot fall on the shoulders of a lone engineer, but one can expect the engineer to issue warnings when a safe exit does not exist or the experiment must be terminated. The only way one can justify continuation of an experiment without safe exit is for all participants (including the subjects of the experiment) to have given valid consent for its continuation.

Let us illustrate by examples what this might involve. Ships need lifeboats with sufficient spaces for all passengers and crew members. Buildings need usable fire escapes. Operation of nuclear power plants calls for realistic means of evacuating nearby communities. The foregoing are examples of safe exits for people. Provisions are needed for safe abandonment of products and materials: altogether too many truck accidents and train derailments have exposed communities to toxic gases, and too many dumps have let toxic wastes get to the groundwater table or into the hands of children. Finally, to avoid business failure may require redundant or alternative means of continuing a process when the original procedure fails. An example would be a computer-based data retrieval system backed up by printed copies of the data, or a water supply backed up by a reservoir.

What we have described is risk management; in other words, how do you go about meeting and minimizing the damage identified in a risk assessment exercise. The last line of defense, and the one which must not be omitted, is the safe exit. A key word in this context is "management." Coordination among producers, users, and local communities are required to provide a realistic safe exit. Engineers are the ideal catalysts to set the process in motion. This is an added burden of responsibility and must be balanced by concomitant rights to openly identify the risks and communicate with other producers and users across organizational barriers.

As we stated in Chap. 2, the responsibility of engineers for safety derives from clients' and the public's right not to be endangered without prior warning in a manner understandable to them. Only with adequate knowledge can persons become willing participants in an engineering project qua experiment, decide not to participate, or decide to oppose it. An ethics based on distributive justice which gives rights to clients (and the public) and to engineers (and their managers) supports this view, but it can also be founded on duty- or goal-based theories of ethical behavior. Engineers need to handle safety issues with great care, but they need not reassess each detail on ethical bases if by habit they have acquired the appropriate "virtues" of responsible engineering.

Study Questions

1 Collect some examples of literature promoting and criticizing use of nuclear power. A good start could be made with Gueron (pro, 1984) and MacKenzie (con, 1984). Are the statements factually complete? Do you find yourself agreeing with what-

ever item you have read last? Discuss the responsibility of experts to reasonably educate the populace about the issues involved, pro and con.

2 It has been said that Three Mile Island showed us the risks of nuclear power and the Arab oil embargo the risk of having no energy. Removing hazardous products or services from the market has been criticized as closing out the options of those with rising aspirations who can now afford them and who may all along have borne more than their share of the risks without any of the benefits. Finally, pioneers have always exposed themselves to risk. Without risk there would be no progress. Discuss this problem of "the risk of no risk." (Compare: Wildavsky, 1980).

3 A number of engineers engaged in nuclear power plant work have expressed their concern over inadequate attention to safety. Some resigned first, then went public with their testimony; some spoke out and were fired; others spoke up but nevertheless retained their positions. Examine the literature about the cases listed below to see if there were any issues of ethical import involved. If so, what were they?

a Carl Houston, 1970, welding superintendent, Stone & Webster (Houston, 1975)

b Peter Faulkner, 1974, systems application engineer, Nuclear Services Corporation (Faulkner, 1981)

c Dale G. Bridenbaugh, 1976, manager of performance evaluation and improvement; Richard B. Hubbard, 1976, manager of quality assurance; Gregory C. Minor, 1976, manager of advanced control and instrumentation; all with Atomic Power Division, General Electric Company, San Jose, California (Kaplan, 1976; Weil, 1977)

d Ronald M. Fluegge, 1976, safety analyst; Demetrios L. Basdekas, 1976, reactor engineer; both with Nuclear Regulatory Commission (*Congressional Record*, 13 Dec 1976)

e Robert D. Pollard, 1976, project manager, Nuclear Regulatory Commission (Friedlander, 1976)

4 Discuss the notion of safe exit, using evacuation plans for communities near nuclear power plants or chemical process plants. Examples (and sample references) you could use include Bhopal's parent plant in Institute, West Virginia (Beck, 1984) and the following nuclear power plants: Diablo Canyon (Gini, 1983), Shoreham (Zorpette, 1987), Seabrook (Larmer, 1987), and early plans for a plant in New York City (Mazuzan, 1986).

5 Search the literature for reports on the Swedish referendum on nuclear power. A popular vote was to be taken after a 1-year public debate on the pros and cons, with proponents and opponents given funds by the government to air their views. Discuss the procedure and its possible applicability in other countries or to other technological issues.

SUMMARY

A *risk* is the potential that something unwanted and harmful may occur. A thing is *safe* for persons to the extent that they judge (or would judge) its risks to be acceptable in the light of full information about the risks and in light of their settled value principles. Thus, in designing for safety, estimates must be made of which risks are acceptable to clients and to the public that will be affected by the projects or products in question.

Many factors influence people's judgments when they decide which risks

are acceptable. Most basic is their set of value principles regarding what they care about and to what extent they care about it. Other factors include whether or not a risk is assumed voluntarily, the degree of anxiety connected with any risk, whether or not a risk is immediately evident, whether or not potential victims are identifiable beforehand, and the manner in which statistics about a risk are presented to people.

Thus, for engineers, assessing safety is a complex matter. First, the risks connected to a project or product must be identified. This requires foreseeing both intended and unintended interactions between individuals or groups and machines or systems. Second, the purposes of the project or product must be identified and ranked in importance. Third, the costs of reducing risks must be estimated. Fourth, the costs must be weighed against both organizational goals (e.g., profit, reputation for quality, avoiding lawsuits) and degrees of acceptability of risks to clients and the public. Fifth, the project or product must be tested and then either carried out or manufactured.

Uncertainties in assessing risks arise at all these stages. For example, at the stage of testing a product only one or a few prototypes are typically used, and at that under carefully controlled conditions. Results may not accurately mirror what will happen following mass production and installation under normal operating conditions. Moreover, testing a product to destruction (the most effective way of testing) is sometimes ineffective or inappropriate. It may only be possible to work with simulations, including analytical tools such as fault-tree analysis (tracing possible causes of a systems failure back to the component level).

In spite of the complexities involved, a great many risks can be reduced or eliminated in fairly obvious and routine ways, at least by those engineers and managers who work with an attitude of deep caution. And increasingly the specter of legal liability serves as an incentive toward a preventive, defensive approach to engineering. Conceiving of engineering as a social experiment helps foster such an attitude. Moreover, by emphasizing the notion of informed consent, the experimentation model points out how safety is ultimately a matter of informed judgment about the acceptability of risks.

If the malfunction of a system can lead to serious injuries, death, and other grave consequences, such a system must be equipped with *safe exit* for those who would otherwise be hurt. Safe termination of an experiment in this sense is good experimental procedure and responsible engineering.