book emphasiz-
niversally pres-

—Carver Mead,
f Engineering and
ute of Technology,
MIT Prize Winner.

f the root causes
ny riveting exam-
enlightening dis-

—David J. Farber,
munication Systems
ces and Professor of
he Wharton School,
sity of Pennsylvania.

ch us an invaluable
eliance on complex
disasters unless we

Brent H. Woodworth,
ponse Team Manager.

MINDING THE MACHINES

PREVENTING TECHNOLOGICAL DISASTERS

William M. Evan

The Wharton School
and
School of Arts and Sciences
University of Pennsylvania

Mark Manion

Program in Philosophy
College of Arts and Sciences
and College of Engineering
Drexel University

ISBN 0-13-065646-1
90000
9 790130 656468

PH
PTR
Prentice Hall PTR, Upper Saddle River, NJ 07458
www.phptr.com

President's Council on Year 2000 Conversion Information Center. Retrieved from the World Wide Web at: www.y2k.gov

Ratajczak, D. (2000). "Although overblown, Y2K preparation paid off," *The Atlanta Journal and Constitution*, January 23: H2.

Sandberg, Jared. (2000). "Why Y2K won't die," *Newsweek*, January 10: 38–39.

Taylor, Paul. (2000). "The surprise benefits of bug-free Y2K," *Financial Times* (London), January 5: B4.

Tenner, E. (1996). *Why things bite back: Technology and the revenge of unintended consequences*. New York: Vintage Books.

Trott, Bob. (1998). "Microsoft wakes up to the Y2K problem," *Infoworld*, 20 (15): 1.

Ulrich, William. (1997). *The Year 2000 software crisis: Challenge of the century*. Upper Saddle River, NJ: Yourdin Press.

Urakami, Leiji. (2000). "U.S. declares victory, defends huge repair costs," *Japan Economic Newswire*, January 3: A1.

CHAPTER 4

Theories of Technological Disasters

"Nothing is so practical as a sound theory"

—Kurt Lewin

The pivotal concept of *technological disaster* seems to be self-evident. In reality, however, its definition is anything but self-evident. Four different theories—systems theory, normal accident theory, high reliability theory, and sociotechnical systems theory—are presented. Our task in this chapter is to clarify the meaning of technological disaster by analyzing these four theories.

A Systems Approach to Technological Disasters

A *closed-systems analysis* treats any technological system as independent of external factors and tends to focus exclusively on internal structural properties and internal relations; analysis of parts of the system is ultimately subordinated to the analysis of the system as a whole. This approach, however, unnecessarily restricts the conception of a technological system because (1) it fails to consider the external environments impinging on the system, (2) it fails to consider the dynamic equilibrium that must be established between the internal and external environments of a system, and (3) it rarely considers changes of the system over time. Because of these defects, the closed-systems approach is not useful in explaining the conditions under which a technological system achieves a "steady state," namely, maintains a balance among opposing variables in a system. Nor does it explain the conditions under which the system errs or deviates in a destructive way from its intended purpose (Cherns, 1978). Because of the defects of a closed-systems approach, we will explore the implications of an *open-systems* approach for understanding technological disasters (von Bertalanffy, 1950; Miller, 1978).

Since all technological systems, from steamboats to petrochemical plants, are consciously designed to achieve a goal or set of goals, a systems definition of technological disaster is based on the observed discrepancies between the goals of the system and its overall performance. In this way, we can understand failures and disasters of technology as shortfalls between performance and standards, or gaps between promise and performance. An operational definition of this kind stresses goals and performance because failures and disasters in technological systems can only be measured against the intended purposes of a system (Turner, 1978).

In a complex technological system, failures and disasters are never due to a single cause. Therefore, in taking a systems approach to technological failure and disaster, it is necessary to take into account the functional context in which a system is operating (Bignell and Fortune, 1984). It is important to point out that a system's disaster is always a major failure of the goals and purposes of a system. Thus, the failure of a system cannot be separated from the intentions of the human beings who design, operate, or manage it. In other words, technological failures and disasters cannot be fully understood unless placed in the context of the social setting in which they occur. Moreover, these general observations apply to the whole continuum of technological systems. Any technological system, no matter how mundane—be it a thermostat, an automobile, a telecommunications satellite, or a large-scale technological system such as an electric utility or a nuclear reactor—exhibit various components functioning in a complex and integrated way as designed by human beings for a particular purpose.

A technological disaster can be understood as a radical departure from the pattern of expected inputs and outputs of a system. It almost always entails the failure of negative feedback to restore the system to a stable or steady state. Negative feedback involves the sensing of information regarding the current state of the system and using the information to achieve the desired balance between the input and output of the system. If there is a sufficient difference between the stated goal of a system and its actual performance, engineers or the mechanisms they have developed seek to reduce the difference. Negative feedback mechanisms, built into the system, are designed to detect and reduce deviations or errors in performance. By driving the controls in the direction opposite to the initial deviation or error in performance, negative feedback maintains the desired state of a system and reduces the discrepancy between the goals of a system and the performance of that system. When signals are fed back over the feedback channel in such a manner that they decrease the deviation of system output from a steady state, we observe negative feedback in operation (Rapoport, 1968).

The operation of a mundane thermostat illustrates the mechanism of negative feedback. The *desired* temperature setting is the goal, and the *recorded* temperature in the room is a measure of the performance of the heating system. If the difference between the desired temperature and the recorded temperature is less than zero, the furnace sends up heat. As soon as the difference in temperature readings reaches a value slightly greater than zero, the furnace is turned off.

The first task of a systems approach is to identify the relevant levels of analysis. Structures at the indicated level of analysis are called *systems*. Those at the level above a given system are called *suprasystems,* and those at the level below are *subsystems*. Complex systems may include several suprasuprasystems and subsubsystems (Miller, 1978). Applying a systems approach to our understanding of disaster involves at least two steps. First, we must identify all the components, subsubsystems, subsystems, systems, suprasystems, and suprasuprasystems thought to be relevant to the problem at hand. Second, we must identify breakdowns in the feedback mechanisms when the entire complex of systems, subsystems, and suprasystems have failed to function in an integrated manner.

These distinctions make it possible for us to make a preliminary distinction between a technological failure and a technological disaster. A failure involves a breakdown of one component and/or one subsystem of a technological system. By contrast, a disaster involves a breakdown of multiple components and multiple subsystems of a technological system, thereby threatening the viability of the entire system. Otherwise put, a technological for countering destructive positive feedback, which should be distinguished from positive feedback effects of a beneficial and self-enhancing nature that amplify deviations in a positive direction (Rapoport, 1968; Evan, 1993). When a corporation that embarks on a new market strategy exceeds its projected growth rate by a significant percentage, it is enjoying positive feedback of a beneficial variety. It is important to point out, in addition, that destructive positive feedback can occur at *any* level of a system, subsystem, or suprasystem.

Systems failures clearly do not involve a concatenation of random events; they require time for destructive positive feedback to emerge. As Turner puts it:

> For each technological failure that emerges. . .there is an "incubation period" before the disaster that begins when the first of the ambiguous or unnoticed events, which will eventually accumulate to provoke the disaster, occurs. . .Large-scale disasters rarely develop instantaneously, and the incubation period provides time for resources of energy, materials, and manpower, which are to produce the disaster, to be covertly and inadvertently assembled. (Turner, 1978: 193)

An influential theory of failure and disaster of technological systems, that of Charles Perrow, takes an explicit systems approach.

PERROW'S THEORY OF "NORMAL ACCIDENTS" (NAT)

Perrow, an outstanding sociologist, analyzes the catastrophic potential of high-risk technologies through what he calls a "systems" analysis. Perrow begins by developing a hierarchy of failure. At the first level, an "incident" can occur, which usually pertains to failures of the smallest components of a system—the parts and units. Accidents tend to occur when an array of parts and units fail, causing multiple subsystems to fail, which, in turn, may cause the entire system to break down. This leads Perrow to define an accident as "a failure in a subsystem, or the system as a whole, that damages more than one unit and in doing so disrupts the ongoing or future output of the system" (Perrow, 1984: 67). Next, Perrow distinguishes between two types of accidents—"component failure accidents" and "systems accidents." These, in turn, are to be distinguished, says Perrow, "on the basis of whether any interactions of two or more failures is anticipated, expected, or comprehensible to the persons who designed the system and those who are adequately trained to operate it" (Perrow, 1984: 70–71). But, Perrow adds, "it is not the source of the accident that distinguishes the two types of accidents because all accidents start with a component failure—a valve or operator error. It is the presence or not of multiple failures that interact in unanticipated ways [. . .that are the distinguishing characteristics]" (p. 71). Perrow concludes that a systems accident is "an unanticipated interaction of multiple failures" (p. 70).

To account for an unanticipated interaction of multiple failures, Perrow distinguishes two critical dimensions along which systems can be classified. According to Perrow, systems can be either "linear" or "complex," or can be either "loosely coupled" or "tightly coupled."

The concept of coupling is well known in engineering and has been adopted as well in the social sciences. As Perrow defines it, *tight coupling* is "a mechanical term meaning there is no slack or buffer or give between two items [in a system]. What happens to one directly affects what happens in the other" (Perrow, 1984: 89–90). The opposite term, *loose coupling,* means the contrary—that there is a lot of slack between components, so when one fails, there is a buffer that allows the system to recover from a perturbation that has sent the system out of control. In a system exhibiting loose coupling, the relative insulation between subsystems slows the negative effects of a localized component mishap from spreading to other, larger units such as subsystems. Tightly coupled systems, on the other hand, need to have all the buffers and redundancies built in to the design and structure of the system itself.

The concept of *complexity* is a term of art used by Perrow to mean "baffling, hidden interactions" not anticipated in the original design that have the potential to "jump" from one subsystem to another (Perrow, 1984: 94). High-risk technologies are complex in that a single component often serves more than one function. To use an example from Perrow, a heat exchanger might be used to both absorb excess heat from a chemical reactor and to heat gas in a certain tank (Perrow, 1984: 79). Perrow suggests that when subsystems share pipes, valves, and feed-lines, and when feedback mechanisms automatically control key processes, accidents are to be expected, even inevitable—and hence "normal." Moreover, components in different subsystems are often in close operational proximity. If a component fails in one subsystem, the disruption might "jump over" into another subsystem, causing unplanned disruptive consequences. What Perrow is attempting to capture with his concept of complexity is what engineers call a *common-mode failure,* a phenomenon well studied in reliability engineering and engineering design science. Common-mode failures are relatively well known to design engineers and, more often than not, are included in safety and risk analysis techniques such as fault-tree and event-tree methods.

For Perrow, technical systems most prone to failure are complex, tightly coupled systems—that is, those technical systems that exhibit many potentials for common-mode failure. In his Normal Accident Theory (NAT), technological disasters are classified as "normal" due to the tight coupling and interactive complexity they exhibit, namely factors that make the chain of events leading to a disaster incomprehensible to the operators.

Perrow attempts to account for technological disasters without appealing to such factors as "operator error, faulty design or equipment, lack of attention to safety features, lack of operating experience, inadequately trained personnel, failure to use the most advanced technology, systems that are under financed, or poorly run" (Perrow, 1984: 63). As he states: "The analysis . . . focuses on the properties of systems themselves, rather than on the errors that owners, designers, and operators make in running them" (p. 63). Hence, human factors appear to play a relatively unimportant role in NAT. It is as if the technologies that concern Perrow have become autonomous—beyond the control of human beings.

It is a fact, however, that many of the accounts of technological disaster chronicled by Perrow in his book *Normal Accidents* concern negligent managers, incompetent operators, shortsighted owners, and disorganized social systems. As Hirschorn points out, Perrow seems to ignore his own evidence that technological disasters are caused by a complex interaction of technical systems, human factors systems, organizational systems, and socio-cultural systems, and not as a result only of tightly coupled, complex technical and organizational systems (Hirschorn, 1985: 846). For example, many of the marine accidents discussed by Perrow were caused by the conscious refusal of captains to cooperate with one another when their ships were in danger of collision (Perrow, 1984: 174). Or, take, for example, what Perrow says in his narrative of the Flixborough chemical plant explosion, which killed 28 people, injured dozens of others, destroyed the plant, and damaged about 1,000 houses, shops, and factories in rural England. Perrow himself concludes that "fairly gross negligence and incompetence seem to account for this accident" (p. 111). To refer to the Flixborough chemical plant as an "accident" is clearly a misnomer. It was a technological disaster.

We can agree with Perrow that the common excuse of operator error is insufficient to account for technological disasters. Such excuses divert attention away from systems failures in Perrow's sense of the term. Such excuses also divert attention away from various human, organizational, and socio-cultural factors that are also at the root of technological failures and disasters. Interactions among operators, technology, and organizations are intrinsically complex; whatever failures occur cannot be blamed solely on operators. By declaring that operators must have failed, complex problems are covered up. As Perrow puts it:

> Finding the faulty designs responsible would entail enormous shutdown and retrofitting costs, finding that management was responsible would threaten those in charge, but finding the operators were responsible preserves the system, with some soporific injunctions about better training. (p. 133)

Perrow is unquestionably correct in this regard. One must see the operators as only one link in the chain. Systems failures should be seen as human-machine mismatches. The behavior of operators cannot alone account for failures because their behavior can only be understood in the context of the equipment they use, the design of the technology, and the administrative structure that controls operators. However, Perrow's marginalization of human, organizational, and socio-cultural factors surrounding the causes of technological disasters leads to an impoverished understanding of the complex dynamics of technological disasters. A comprehensive theory of technological disasters must focus on the complex effects of technical, human, organizational, and socio-cultural factors that cause technological disasters, in addition to such structural factors as interactive complexity and tight coupling.

It is noteworthy that, prior to the publication of his influential book *Normal Accidents,* Perrow himself outlined the rudiments of such a theory of technological disaster in an article

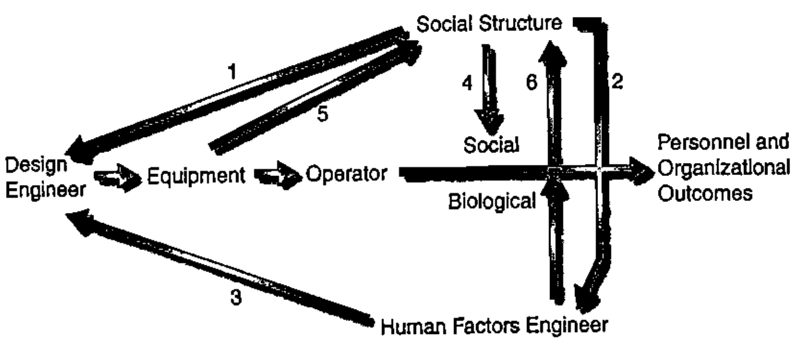


Figure 4–1
Perrow's "The Context of Design."
Source: Reprinted from "The organizational context of human factors engineering," by Charles Perrow published in *Administrative Science Quarterly* Volume 28, Number 4 (December 1983) by permission of Administrative Science Quarterly.

entitled "The Organizational Context of Human Factors Engineering" (Perrow, 1983). In this article Perrow accords a significant role to sets of interrelationships between operators, design engineers, and human factors engineers, as shown in his model, which is reproduced in Figure 4–1.

Perrow analyzes the various sets of interrelationships between the human factors engineer, the design engineer, the social structure, etc., as illustrated in lines 1 through 6.

In fact, Perrow identified four factors of organizational design that influence engineering design:

1. top management goals and perspectives
2. the reward structure of the organization
3. insulation of design engineers from the consequences of their design decisions
4. aspects of social structure

Perrow argues that goals such as speed, power, and maneuverability usually win out over considerations of easy maintenance, ease of operation, reliability, and sometimes safety when choosing among various designs (Perrow, 1983: 521). In addition, top management often fails to see the utility of a broader conception of technological design. The authority structure—whether it is centralized or decentralized, or the span of control over operational procedures is tight or loose—also impinges on the design of hardware. As Perrow puts it:

> The design of systems, and the equipment that is used, is not entirely determined by technical or engineering criteria; designers have significant choices available to them that will foster some types of social structures and operator behaviors rather than others. Designers can choose, or they can implicitly accept, design rather than operating criteria, or the criteria implicitly preferred by top management. (1983: 534)

According to Perrow, design engineers have much to learn from human-factors engineers. Design engineers must pay attention to the way "things"—equipment, layout, ease of operation and maintenance—interact with human operators. As he puts it:

> This is especially necessary as the high-demand load of modern technologies threatens to exceed the physical, biological, and cognitive capacities of human operators. For example, passive-monitoring designs encourage de-skilling, tedium, and low system comprehension, which may lead to low morale, low output, and lack of skills to deal with operational problems. (1983: 522)

Hence, Perrow argues that the human-factors engineer "can bring to the design engineer knowledge about anthropometric limits, visual and motor sensitivity, response time, cognitive capacity and memory limits, and workload capacity for individual workers" (1983: 525), all of which may greatly reduce the friction between humans and machines operating within a system.

Perrow's general thesis regarding these relationships is that design engineers and top management fail to take into account relevant information that could be supplied by human-factors engineers regarding the physiological, affective, and cognitive properties of human operators, and their effects on the organization in which the technology is embedded.

According to Perrow, a major deficiency is the design engineer's inability to appreciate the vulnerabilities of human operators. For Perrow, design engineers have a tendency to see technical systems as "closed systems," that is, as systems composed of various hardware components, which are in turn designed as "expert" systems, with absolute rationality and error-free internal logic. In contrast, human beings exhibit "bounded rationality," they have substantial cognitive limits on rationality (Simon, 1957: 38–41). Yet the system design is not responsive to the "bounded" rationality of human operators. Psychological research (Tversky and Kahneman, 1974) and Perrow's own graphic account of accidents (Perrow, 1984) indicate that human operators exercise selective attention, engage in limited search behavior, and discount nonconfirming information when confronted with novel or emergency situations.

The operator is not simply a transfer device in the loop, but a creative interpreter of phenomena, a "bio-cognitive" creature with limited rationality. The design engineer (and the whole organization) should model creative operators in all their complexity more accurately, because the design employed will elicit some, rather than other, performance characteristics of the system. Perrow concludes that design engineers must pay attention to the way technological artifacts are shaped by the organizational structure and by top management interests, which, in turn, shape operator behavior.

Perrow's context of design model (Figure 4–1) is more complex than his later model, articulated in his book *Normal Accidents*, where human and organizational factors tend to be de-emphasized. However, the earlier model is still in need of refinement. For one thing, Perrow's model does not include socio-cultural factors, which consist of values and beliefs of the social institutions of the environing society. The engineers and managers who incorporate these values and beliefs exert an impact on the technological system and its management structure. An improved model would include the impact of human-factors engineering on operator behavior, as well as the impact of socio-cultural factors on managers and design engineers. In Figure 4–2, we present a modified version of Perrow's model.

Top managers, who have internalized socio-cultural factors, use the chain of command to direct the behavior of design engineers, human-factors engineers, and operators. Staff personnel, design engineers, and human-factors engineers do not have the authority to direct the behavior of operators; at best they instruct and advise the operators. If and when the suggestions of design and human-factors engineers are challenged by the operators, top management intervenes to resolve the conflict.

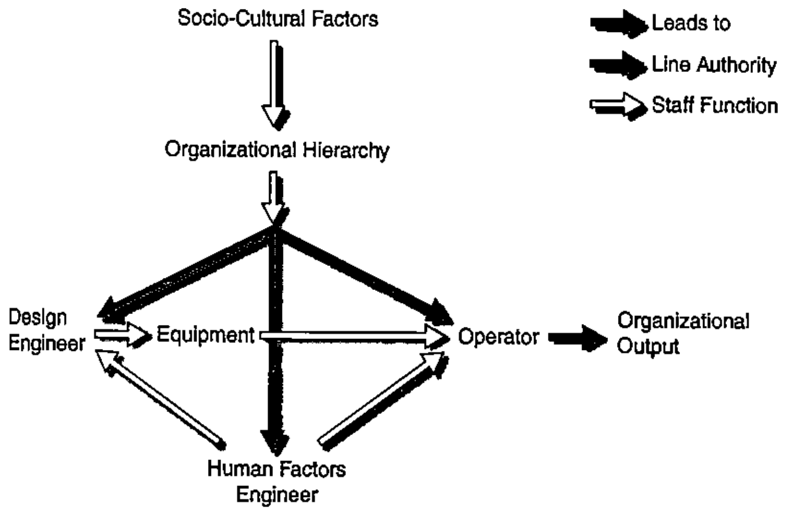


Figure 4–2
Evan and Manion's revised model of Perrow's "The Context of Design."

The hierarchical structure of a technological system provides "different contexts for understanding the system and different incentives to guide action" (Burns and Dietz, 1992: 212). The design engineer is concerned principally with designing a functional, safe, and efficient system; his or her supervisor focuses on productivity and the cohesion of the work team, which may impede monitoring and auditing performance. In addition, top management is understandably oriented to the firm's profitability and shareholder returns on investment.

Notwithstanding our revised model of Perrow, as depicted in Figure 4–2, his overall theory of normal accidents tends to be pessimistic, maintaining that accidents in high technology industries are "normal," in the sense of "expectable," because complex technologies have "outrun our organizational abilities to manage and control them" (Bierly and Spender, 1995: 639). For Perrow, failures are inevitable because organizational powers are unable to handle the safe and reliable design, development, and management of high-risk technologies.

Perrow concludes that the bureaucracy model of organization is inadequate to handle the complexities of modern technology. But, rather than discard the bureaucracy model, which he argues is the best model for managing technology in complex systems, Perrow concludes that human beings cannot successfully manage certain high-risk technologies. But why? Perhaps we can develop

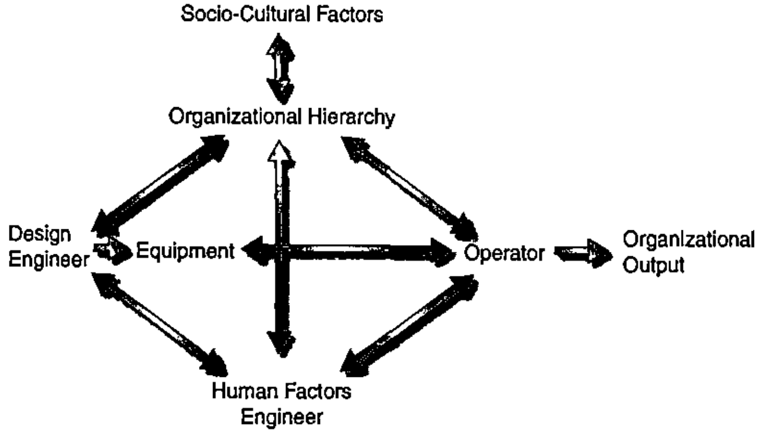


Figure 4–3
Evan and Manion's nonhierarchical consultative model of technological systems.

a nonbureaucratic model of technology management. Figure 4–3 presents the outlines of such a model.

The two-directional arrows between staff and line underscore the need for a *nonhierarchical and consultative relationship,* at least in the planning stages and general operational processes. Two-way flows of communication are especially essential in technological systems to maximize the sharing of information among all personnel regardless of position in the organizational hierarchy. Bureaucratic barriers to cooperation are particularly dysfunctional, given our limited understanding of technological systems and our limited ability to control them. However, when a crisis arises in the operations of a technological system, the command model—namely, an hierarchical and single-directional mode of communication—would supersede the nonhierarchical consultative model in an effort to contain the crisis and limit the damages.

Perrow's analysis of technological failures in *Normal Accidents* narrowly restricts analysis of the causes of technological disaster to technical and organizational factors—for example, the effects of complexity and coupling—and downplays human and socio-cultural factors. We propose, instead, a *concentric* model of technological systems that takes into account human and socio-cultural factors as well as technical and organizational factors. The difference between Perrow's model and ours is represented in Figure 4–4.

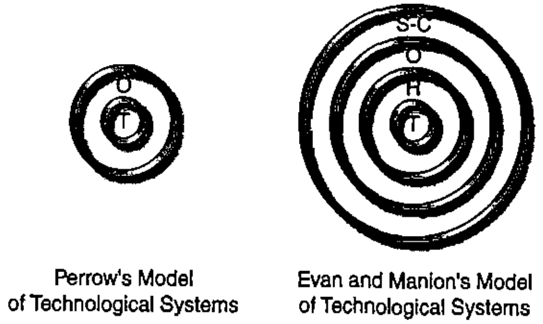

O
T
S-C
O
H
T
Perrow's Model of Technological Systems
Evan and Manion's Model of Technological Systems

Figure 4–4
Perrow's model of technological systems versus Evan and Manion's model of technological systems.

Organizational factors are often left implicit in NAT (Perrow, 1999: 368). For example, in analyzing the paradoxes of organizational design in high-risk systems, Perrow suggests that we have reached a cultural and organizational cul-de-sac (Perrow, 1984: 360). According to Perrow, we need centralized systems to ensure obedient responses in emergencies, but we also need decentralized systems so that workers can use their initiative to help solve unexpected problems. For Perrow, combining centralization and decentralization is impossible in tightly coupled, highly complex systems. This is because systems that exhibit tight coupling require increased centralization to facilitate rapid, authoritative, and correct decision making; whereas systems, which exhibit interactive complexity, require decentralization of decision-making authority. His underlying assumption is that our administrative capabilities are decidedly inadequate to manage high-risk technologies. However, models of organizational control can be both centralized and decentralized. In fact, as any proponent of the sociotechnical school of management will readily point out, many manufacturing organizations are designed according to "sociotechnical principles" in which close coordination is achieved between workers and work teams without resorting to hierarchy (Pasmore and Sherwood, 1978).

Perrow, however, is strongly committed to the superiority of the bureaucratic model, despite its limitations. In fact, he claims that:

> Bureaucracy is a form of organization superior to all others we know and can hope to afford in the near or middle future; the chances of doing away with it or changing it are probably

> non-existent in the West in this century. Thus it is crucial to understand it and appreciate it. But it is also crucial to understand not only how it mobilizes social resources for desirable ends, but also how it inevitably concentrates those forces in the hands of a few who are prone to use them for ends we do not approve of, for ends we are not generally aware of, and more frightening still, for ends we are led to accept because we are not in a position to conceive alternative ones. (1979: 7)

Perrow finds himself on the horns of a dilemma primarily because he does not consider any other form of organizational control. The only model he considers is the standard bureaucratic structure. Since bureaucratic principles are ultimately unsuccessful in combining loose and tightly coupled structures, or centralized and decentralized authority, he concludes that high-risk technology cannot be safely and reliably developed and managed. Perrow does direct our attention to a significant problem that needs to be addressed, but other models of organizational design are available, such as those identified in the literature on high reliability organizations.

High Reliability Theory (HRT)

In the closing chapter of his book *Normal Accidents,* Perrow classifies high-risk systems into three categories: (1) systems that should be abandoned because the risks outweigh any potential benefits; (2) systems that could be made less risky or those with potential benefits such that some risks should be tolerated; and (3) systems that are to some extent self-correcting and could be further improved. Technologies of the third category include mining, aircraft, dams, and chemical plants. Technologies in the second category include marine transport and genetic engineering. Nuclear weapons and nuclear power fall into his first category of technologies that cannot be tolerated because they are too prone to "systems" accidents; in other words, their failure is immanent and inevitable—"normal."

Perrow's prudent and circumspect conclusions regarding high-risk technological systems stimulated other researchers to study high-reliability organizations (HROs) such as nuclear submarines, nuclear-powered aircraft carriers, nuclear power plants, and air traffic control centers. These organizations are "characterized by both advanced technology . . . and a high degree of interdependence . . . " (Roberts, 1990 [a]: 161).

Roberts and her interdisciplinary team of researchers studied three HROs to ascertain "how they maintain safe and reliable operations under hazardous conditions" (Roberts, 1990 [b]: 102). The three organizations included the Pacific Gas and Electric Company (PG&E), the Federal Aviation Air Traffic Control system, and a U.S. Navy aircraft carrier. Each of these organizations involved technologies exhibiting Perrow's complex interaction and tight coupling characteristics. Nevertheless, their performance was highly reliable: PG&E, a utility serving 4 million customers in California, was 99.96 percent reliable in terms of outages; air traffic control centers had not had a single mid-air collision in the 10 years preceeding the study; the U.S. Navy aircraft carrier "crunch rate" (accidents of aircraft being moved on deck) in 1989 was one in 8,000 moves; and the fatality rate due to deck fire in 1989 on aircraft carriers was 2.97 for every 100,000 hours of flight time (Roberts, 1990 [b]: 102–103).

Another striking example of an HRO is the Diablo Canyon nuclear power plant operated by PG&E. This plant is capable of generating 2,190 megawatts (MW) of electricity. Plant personnel include operations, maintenance, engineering, administration, and/or technical, totaling 1,250 employees on site, plus more than 1,100 outside consultants.

In stark contrast, PG&E also operates a conventional fossil-fueled steam generating plant near Pittsburg, California. The plant produces roughly the same amount of electricity with one-fourth of the personnel of the Diablo Canyon plant. Its budget for operations and maintenance in 1990 was $30,318,000, whereas the budget of the Diablo Canyon facility was $187,000,000. The difference in operating costs of the two plants—one is six times more expensive than the other—is due to "the added complexity of nuclear technology, the current political and regulatory climate surrounding nuclear power generation, and specific organizational strategies adopted for the management of this technology at Diablo Canyon" (Schulman, 1993: 356).

The impressive performance record of HROs in this study was achieved by systematically applying strategies to counter the potential hazards associated with technological complexity and tight coupling. Among the organizational strategies and processes identified are continuous training of personnel, job redesign, and redundancy (Roberts, 1990 [a]). Another strategy is building-in a "culture of reliability," norms and values pertaining to safety, accountability, and responsibility. "Managers of HROs must confront the cost of potential catastrophe and build into their organizations strong norms for cultures of reliability" (Roberts, 1990 [b]: 112).

In their study of a nuclear submarine, Bierly and Spender (1995) underscore the contributions of Admiral Hyman Rickover, the creator of the U.S. nuclear navy, to the unique culture of this type of organization. Insisting on stringent recruitment standards, Rickover personally interviewed each potential officer. His principles of selection—apart from the highest level of professional competence—were commitment, trust, communication, and performance under pressure. Along with his unique approach to the selection and training of naval reactor officers, his "obsession with safety" affected the design, manufacture, and operation of the nuclear power plant. Rickover "forced contractors to approach their task with the same demanding zero-defect engineering standards that builders of supersonic fighters had used for years" (Bierly and Spender, 1995: 652).

As of 1979, when the Three Mile Island (TMI) accident occurred, Rickover had been managing 152 naval reactors, operating almost 30 years without a *single* accident resulting in radioactive emissions. In the course of the TMI inquiry, Rickover "insisted that this extraordinary reliability was not due to the military context and personnel, rather that it was due to careful selection of highly intelligent and motivated people who were thoroughly trained and then held personally accountable" (Bierly and Spender, 1995: 651). If all managers of nuclear power plants around the world had Rickover's dedication to reliability, safety, and professional discipline of their employees, the safety records of such plants would be greatly enhanced. Rickover's conception of a culture of reliability entailed the following components:

> . . .each individual's ownership of the task, responsibility, attention to detail, high professionalism, moral integrity, and mutual respect created the cultural context necessary for high quality communications under high risk and high stress conditions. Communication and recommendations can flow upward from the crewmen to the officers as well as downward. Likewise communication about all kinds of mistakes, operational, technical or administrative, can flow rapidly through the system. Anyone making a mistake can feel free to report it immediately so that the watch officers can really understand what is happening to the system. Rickover believed that the real danger lay in concealing mistakes, for when this happens those in charge become disconnected and disoriented. This could be disastrous in the high-risk circumstances of a nuclear warship. (Bierly and Spender, 1995: 651)

Perrow's NAT has reified "technological systems" to the point that no human operators or agents can ever be held accountable or responsible for any system failure. This impersonal conception of systems fails to account for the fact that some high-risk systems are highly reliable, presumably because motivating human operators makes a difference in reducing the vulnerability of systems to failure. The research of Roberts and her colleagues in high-reliability organizations, as well as Rickover's experience with nuclear submarines, evidently do not fit Perrow's theory: ***interactive complexity and tight coupling need not result*** *in catastrophe.*

As Roberts and her colleagues have shown in their work on HRT, and as Rickover has dramatically established, the principal characteristics of high-reliability organizations are (1) top management's commitment to safety as an organizational goal, (2) the need for personnel redundancy as well as engineering redundancy, (3) the development of a culture of reliability, and (4) the valuation of organizational learning (Sagan, 1993). When these principles are implemented, they have the effect of countering the potentially catastrophic consequences of interactive complexity and tight coupling that Perrow's theory predicts.

Perrow's analysis reminds us that corporate elites have constructed our technologies and that we can abandon them if they become oppressive. They are indeed social constructions (Perrow, 1984: 285). Yet, he simultaneously evokes a picture of "transcendental technologies" that defy our capacities to organize and manage technology.

A Sociotechnical Systems Analysis of Technological Disasters

As we have seen, Perrow's model suggests that the dynamics of technological failure and disaster are a result of interactive complexity and tightly coupled systems. However, the model we are advancing will demonstrate that, in addition to the structural features of interactive complexity and tight coupling, the dynamics of technological failure and disaster reflect fundamental problems of organization design, worker competence, management systems, and the socio-cultural context in which the technology develops.

On Perrow's account, design engineers are incapable of anticipating all of the possible effects of complex systems and, hence, failure is inevitable. But, technological systems are human constructions ultimately under the control of human beings. People *can* modify them to minimize and possibly eliminate errors if they are so motivated. As Perrow himself states, "ultimately, the issue is not risk, but power, the power to impose risks on the many for the benefit of the few" (Perrow, 1984, p. 306). Hence, the causes of the risks and harms posed by technology are more of an organizational structure issue than those associated with the abstract system itself.

In contrast to organizational designs that focus on either the social system or the technical system exclusively, the *sociotechnical systems approach* integrates the demands of both. Emery (1959) referred to this dual concern with the social and technical systems as *joint optimization*. A sociotechnical systems approach focuses attention on dynamic processes within organizations and between organizations and their environments.

For complex, hazardous technologies, one major cause of loss of control is the failure of both design engineers and organizational planners to incorporate adequate sociotechnical detection and monitoring systems that feed back observable deviations between the sociotechnical system and its external environment. According to E.L. Trist, sociotechnical systems breakdowns almost always "reflect the mutual permeation of a particular organization and its environment that is [often] the cause of such imbalance" (Trist, 1978: 45). Creating high-reliability, high-performance sociotechnical systems requires analyzing the *interdependencies* among the social, technical, and environmental subsystems that render each system unique. With this approach, the emphasis is more on interdependencies between the technical and social subsystems rather than on isolated problems. The gap between the technical systems analysis and the social systems analysis leads to a frequent lack of coordination between the builders and designers of the systems (technical system) on the one hand and the operators and managers of the system (social system) on the other. This leads to "different people working in very different contexts and according to different rules with different constraints" (Burns and Dietz, 1992: 212).

Thomas Hughes, a distinguished historian of technology, articulates a systems approach in his writings. Hughes's analysis focuses on what he calls "large-scale technological systems." This approach stresses the importance of paying attention to the different but interlocking elements of physical artifacts, institutions, and their environments, thereby integrating the technical, economic, social, and political aspects of technological development. As Hughes puts it:

> Technological systems contain messy, complex, problem solving components. They are both socially constructed and socially shaping. Among the components in technological systems are physical artifacts, such as turbo generators, transformers, and transmission lines in electric light and power systems. Technological systems also include *organizations*, such as manufacturing firms, utility companies, and investment banks, and they incorporate components usually labeled scientific, such as books, articles, and university teaching and research programs. Legislative artifacts, such as regulatory laws, can also be part of technological systems. Because they are socially constructed and adapted in order to function in systems, natural resources, such as coalmines, also qualify as system artifacts. (Hughes, 1994: 51)

The work of Hughes draws attention to the socially constructed nature of technological systems. After all, sociotechnical systems *are* constructed by individuals and collectivities (Latour and Woolgar, 1986). Since different stakeholders or constituents have different, often conflicting interests and resources, they tend to differ in their views as to the proper structuring and design of technological systems. In addition, different stakeholders may have different and competing processes for determining what ought to be the proper operation of a technological system (Barnes, 1974). From this perspective, an explanation of technological failure and disaster depends on two factors. The first is the study of the socially constructed conditions of technological development. Because different stakeholders often have competing definitions as to the problems to be solved in determining the best design of a technological system, there needs to be much negotiation and interpretative flexibility in design decisions (Barnes, 1982).

Second, various stakeholders will decide differently not only about the definition of the "best" design, but also about the "steady state" of the system in operation. Accordingly, decision making concerning the steady state of a sociotechnical system must be explained by referring to the varied and often competing social and economic interests attributed to the various stakeholders concerned and their capacity to mobilize forces in the course of debate and controversy (Latour and Woolgar, 1986). Social constructivists often talk of this process as one of "closure," which is ultimately achieved when debate and controversy about either the design or the operation of a system is resolved (Bloor, 1976). The merits of a social constructivist approach to technological disaster are clear. Many design decisions about the structure of sociotechnical systems are arrived at in the course of debate and achieve their final form when a stakeholder imposes its solutions on other interested parties by one means or another; that is, by compromise, persuasion, or fiat.

Ultimately, the question we confront is not *why* things come apart in one specific instance but *what* in general constrains the capacity of human beings to manage and control complex and potentially harmful technologies. A sociotechnical approach to technological disaster attempts to provide an answer to this question. Moreover, if we accept, with Thomas Hughes, that technical systems are at the same time economic, social, and political constructs, then a systems approach to technological disasters must struggle with this complex web of relationships between technical, economic, social, and political factors.

The preceding analysis leads us to the following operational definition:

A *technological disaster* is a crisis that threatens the viability of a sociotechnical system, which includes machines, design engineers, human operators, rules and role behaviors, and socio-cultural factors, and which results in the massive loss of life, property damage, or environmental deterioration. By contrast, a technological failure, as we indicated in Chapter 1, is defined as the unanticipated breakdown of one or more components of a technological system that may impair its functioning and that may cause minor property damage or loss of life.

CONCLUSION

Technological disasters are failures of sociotechnical systems. This fact should lead design engineers to examine not only the failures of technical design but also the impact of human, organizational, and socio-cultural factors. The hypothesis we are advancing is that those who design and operate sociotechnical systems must concern themselves not only with technology as merely a material artifact but also with the ways in which the hardware and the software are related to economic, social, and political interests of various stakeholders.

The performance, stability, and reliability of sociotechnical systems, as well as their ability to tolerate environmental disturbances, are dependent upon the nature, formation, and interaction of human and socio-cultural subsystems and suprasystems, not simply upon the technical and organizational facets of systems, as Perrow's model suggests. Each sub- and supra-system forms a link in a complex chain. Each has a role in the overall performance of the system. Disturbances in one link can affect the overall integrity of the system. In fact, many of the large-scale technological disasters, discussed in Chapter 8, have been caused by nontechnical factors, namely, the human, organizational, and socio-cultural factors (Meshkati, 1991).

Given that sociotechnical systems are socially constructed, they can be designed and redesigned to minimize the probability of technological disaster. This concept is clearly compatible with High Reliability Theory (HRT). As for Normal Accident Theory (NAT), Perrow sets forth three categories of systems: (1) systems that should be abandoned because the risks outweigh the benefits (2) systems that should be made less risky, and (3) systems that are self-correcting and could be further improved. Underlying Perrow's last two categories is an assumption that it is feasible and desirable to redesign systems to minimize risk. By focusing on the challenge of redesigning sociotechnical systems to minimize risk, we can potentially bridge the theories of HRT and NAT. In the Afterword to his new edition of *Normal Accidents* (1999), Perrow himself envisions the possibility of bridging these two theories (p. 372).

To provide such integration, Ackoff's "interactive idealized design" may be helpful (Ackoff, 1994: 79–81). A renowned systems theorist and operations researcher, Ackoff's design system must fulfill three requirements: technological feasibility, operational viability, and capability of learning from its own experience and "adapting to internal and external changes." To formulate an idealized design requires the participation of "all the systems' current stakeholders, or their representatives" (Ackoff, 1994: 80).

By accepting the primacy of system safety as a fundamental value, idealized system designers may be guided by the principle of minimizing risk. For top management, with a short-time horizon, efficiency all too often trumps safety. By focusing on net returns for the next quarter, they may, however, subject the corporation to design decisions that will prove vulnerable to technological disasters, and hence, to costly losses, such as we witnessed in the Challenger disaster.

To avoid error-inducing designs, idealized system designers build-in a multiplicity of negative feedback mechanisms. In addition, given that tight coupling and interactive complexity increase the risk of failure, idealized system designers should explore the possibility of re-designing sociotechnical systems so that they loosen the coupling and simplify system complexity—even if such system characteristics diminish efficiency in some measure.

In sum, the sociotechnical systems approach to technology, when informed by Ackoff's interactive idealized design process, contributes to our understanding of technological disaster in at least two ways. First, as the work of Hughes and his followers demonstrates, many failures of technology can only be understood when interrelated with a wide range of nontechnological and specifically social and cultural factors. Second, only a sociotechnical systems approach can do justice to the complex set of causes of technological disaster.

We now turn in the following chapter to a discussion of the root causes of technological disaster.

References

Ackoff, R.A. (1994). *The democratic corporation.* New York: Oxford University Press.

Barnes, B. (1974). *Scientific knowledge and sociological theory.* London: Rutledge and Kegan Paul.

Barnes, B. (1982). *T.S. Kuhn and social science.* London: Macmillan.

Bierly, P.E., and Spender, J.C. (1995). "Culture and high reliability organizations: The case of the nuclear submarine," *Journal of Management* 21: 639.

Bignell, V., and Fortune, J. (1984). *Understanding systems failures.* England: Manchester University Press.

Bloor, D. (1976). *Knowledge and social imagery.* London: Routledge and Kegan Paul.

Burns, T.R., and Dietz, T. (1992). "Technology, sociotechnical systems, technological development: An evolutionary perspective." In M. Dierkes and U. Hoffmann (Eds.), *New technology at the outset: Social forces in the shaping of technological innovation.* New York: Campus Verlag.

Cherns, A. (1978). "The principles of sociotechnical design." In W. Passmore and J. Sherwood (Eds.), *Sociotechnical systems: A sourcebook.* San Diego, CA: University Associates: 61–67.

Emery, F. (1959). *Characteristics of sociotechnical systems.* Document No. 527. London: Tavistock Institute.

Evan, W.M. (1993). "Organization theory and organizational effectiveness." In *Organization theory: Research and design.* New York: Macmillan: 369–389.

Hirschhorn, L. (1985). "Normal accidents," *Science* 228 (2).

Hughes, T.P. (1994). "The evolution of large technological systems." In W. Bijker, T. Hughes, and T. Pinch (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology.* Cambridge, MA: MIT Press.

Khandwalla, P. (1977). *The design of organizations.* New York: Harcourt Brace Jovanovich Publishers.

Landau, M. (1969). "Redundancy, rationality, and the problem of duplication and overlap," *Public Administration Review* 29 (4): 346–358.

Latour, B., and Woolgar, S. (1986). *Laboratory life: The social construction of scientific facts.* London: Sage Press.

Meshkati, N. (1991). "Human factors in large-scale technological systems' accidents: Three Mile Island, Bhopal, Chernobyl," *Industrial Crisis Quarterly* 5: 133–154.

Miller, J.G. (1978). *Living systems.* New York: McGraw-Hill.

Pasmore, W., and Sherwood, J. (Eds.). (1978). *Sociotechnical systems: A sourcebook.* San Diego, CA: University Press Associates.

Perrow, C. (1979). *Complex organizations: A Critical Essay.* New York: Scott, Foresman and Wadsworth.

Perrow, C. (1983). "The organizational context of human factors engineering," *Administrative Science Quarterly* 28: 521–541.

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies.* New York: Basic Books.

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies* (2nd ed.). Princeton, NJ: Princeton University Press.

Rapoport, A. (1968). "A philosophical view." In J.H. Milsum (Ed.), *Positive feedback: A general systems approach to positive/negative feedback and mutual causality.* New York: Pergamon Press.

Roberts, K.H. (1990a). "Some characteristics of one type of high reliability organization," *Organization Science* 1: 161.

Roberts, K.H. (1990b). "Managing high reliability organizations," *California Management Review* 32: 102.

Sagan, S. (1993). *The limits of safety: Organizations, accidents, and nuclear weapons.* Princeton, NJ: Princeton University Press.

Schulman, P.R. (1993). "The negotiated order of organizational reliability," *Administration and Society* 2: 356.

Simon, H. (1957). *Models of man: Social and rational.* New York: John Wiley & Sons.

Trist, E.L. (1978). "On socio-technical systems." In W. Passmore and J. Sherwood (Eds.), *Sociotechnical systems: A sourcebook.* San Diego, CA: University Associates: 43–58.

Turner, B. (1978). *Man-made disasters.* London: Wykeham Publications.

Tversky, A., and Kahneman, D. (1974). "Judgment under uncertainty: Heuristics and biases," *Science* 185 (4): 1124–1130.

von Bertalanffy, L. (1950). "The theory of open systems in physics and biology," *Science* 111: 23–29.

Wenk, E. (1989). *Tradeoffs: Imperatives of choice in a high tech world.* Baltimore, MD: The Johns Hopkins Press: 6.

CHAPTER 5

The Root Causes of Technological Disasters

> *"No one wants to learn by mistakes, but we cannot learn enough from successes to go beyond the state of the art."*
>
> —Henry Petroski

What are the causes of technological disasters? It would be a great comfort if we were able to identify a single cause, for that would simplify the development of a preventive strategy. Instead, we must resign ourselves to searching for multiple causes of disaster and hence for multiple strategies for assessment, management, and prevention. Analyzing the causes of technological disaster is of theoretical as well as practical significance. Pursuing our discussion of the previous chapter on sociotechnical systems, we will now focus on two systemic dimensions in an effort to throw light on the causes of technological disaster: (1) internal vs. external systemic factors and (2) technological systems vs. social systems.

In Figure 5–1 we combine these dimensions in a 2 × 2 matrix, yielding four categories of technological disaster, which we will discuss in this chapter. These factors are highly interpenetrating, often have unclear boundaries, and exert mutual influence on each other. The close study of technological disasters reveals that there are often multiple causes of disaster. In practice it may be difficult to isolate a single cause—technical design factors, human factors, organizational systems factors, or socio-cultural factors—because many technological disasters are the result of a combination of such causes. Nevertheless, the identification of the four root causes of technological disasters provides a diagnostic tool with which to analyze such disasters.

	Internal Systemic Factors	External Systemic Factors
Technological Systems	Technical Design Factors	Human Factors Factors
Social Systems	Organizational Systems Factors	Socio-Cultural System Factors

Figure 5-1
Systemic dimensions underlying the causes of technological`disasters.

The assumption underlying this matrix is that we are setting forth a mutually exclusive and jointly exhaustive classification o disasters. For analytic purposes this assumption may further ou understanding of the problem, but it may pose empirically verifi able difficulties. For example, the possible failure of future tech nologies such as recombinant DNA and nanotechnology might b associated with causes that have yet to be anticipated.

TECHNICAL DESIGN FACTORS

Design engineers are constantly working under constraints suc as limited data on the properties and reliabilities of the variou materials they use. Information about the operating conditio under which the materials and pieces of equipment will be ex pected to function is often absent, so that estimates of the resul ing stresses and strains on materials are sometimes little mo than informed guesses.

It is often assumed that science and technology are fully int grated. If this were true, the design engineer would be complete confident in his or her design decisions. Yet all too often scienti theory is not available to ground technological decision makin Therein lies one of the root causes of technical design errors. F thermore, even if all information about those components we

available, the existing physical, chemical, and engineering theories may not yield an unequivocal solution to a design problem.

Examining R.R. Whyte's 1975 anthology of case studies of design and equipment failure, a first of its kind, reveals many similarities among various case studies of engineering design failure from which significant generalizations can be drawn (Whyte, 1975). Whyte's book presents a wealth of case studies concerning engineering design failures, including jet and automobile engines, industrial plant turbines and generators, boilers, heat exchangers, metal fatigue, and stress. Most of these failures are related either to uncertainties in the materials used or in the application of the design in question.

Turner's extensive review of the cases presented in Whyte's book reveals three classes of technical design failures (Turner, 1984: 19–23). The first class of design failures involves designs that extend beyond the knowledge or experience of the designer and that stretch the limits of the previous design. These types of failures are usually the result of "scaling up" existing satisfactory designs to achieve operational parameters beyond the original design. Engineers call this situation *incremental design*. An example of such a failure is when design engineers use an existing plan for a larger version of a well-tested design, introducing factors that were not anticipated in the original. Other failures are the result of just the opposite: the scaling-down of existing satisfactory designs. Engineers call such practices *streamlining* and *fine-tuning*. Starbuck and Milliken (1988) argue convincingly that 24 previous successful flights had created such confidence at NASA that they began systematically "fine-tuning" the technology and design of the space shuttle Challenger and its rockets until it "broke." As Dumas puts it, "being too ready to extrapolate well beyond previous experience is asking for trouble" (Dumas, 1999: 235). Dumas cites as an example the rapid development of commercial nuclear power plants during the 1960s and 1970s, where, within a few years of constructing the first commercial nuclear power plant, plants six times the size of the original design were built.

A second class of design failures arises when designs are forced to operate under conditions that will ultimately lead to a much wider range of unknown variations and fluctuations of stress. This is the well-studied relationship between static loads and dynamic loads. Many design failures are caused by engineers who failed to take into account variations in dynamic loads, the actual fluctuations and perturbations that will be exerted on a technological system—from a bridge to a piece of copper wiring. Perhaps the most famous case in this category is the collapse of the Tacoma Narrows Bridge in 1940. The design engineers did not take into account the excessive wind over the Narrows—a dynamic load that proved catastrophic. This case demonstrates the importance of taking wind aerodynamics into account in designing a bridge.

A third class of failures concerns uncertainties in the nature, quality, and manufacture of the materials necessary for the design to become a reality. For example, Martin and Schinzinger (1996) recommend that variations from the standard quality of a given grade of steel should be taken into account in the design process. According to these researchers, the design engineer needs to realize that a supplier's data on items like steel, glass, and other materials apply to statistical averages only (Martin and Schinzinger, 1996: 143). Individual components can vary considerably from the mean.

In order to cope with the various uncertainties about materials and components, as well as incomplete knowledge about the conditions under which the products they design actually operate, engineers have traditionally introduced *factors of safety* into their designs to cope with as many unanticipated problems as possible. Factors of safety are intended to prevent problems from arising when stresses from anticipated loads ("duty") and stresses the designed product is supposed to withstand ("capability") depart from their expected values (Nixon and Frost, 1975: 138). A product is considered safe if its capability exceeds its duty. Determining the maximum stress a material must undergo in a particular application and then designing the product to withstand, for example, double that maximum stress load would result in a factor of safety of two. In his books, *To Engineer Is Human* (1985) and *Design Paradigms: Case Histories of Error and Judgment in Engineering* (1994), the engineer Henry Petroski catalogues and discusses case after case of design failures caused by unanticipated stresses, fatigue, problems with static vs. dynamic loads, and uncertainties about materials. He then develops a theory of engineering design through the study of structural, materials, and electrical failures.

Glegg, a lecturer in electrical engineering at Cambridge University, has also tellingly addressed the engineer's problem of margin of safety:

> We all automatically insure against risks, often very remote ones. Everyone takes out a policy against fire destroying a new house, which fortunately is a rare occurrence.
>
> By contrast, the insurance of a new design against much less remote disasters is not so automatic. Temperature stresses, torsional vibration, feedback oscillations and similar destroying forces may break out without warning with devastating results. Nearly all machines have some potential disaster lurking in the background. . . . The best protection is a large margin of safety. . . . Develop as large a safety margin as you can against such things as laziness, impatience, prejudice, and arrogance and all the other human failings that inhibit constructive achievement. . . . of creative engineering design. (Glegg, 1971: 88, 93)

A fourth category of failure, which Whyte does not address, pertains to inadequacies in the proper testing and/or prototyping of technological products or processes. There are limitations to the testing process itself, for sometimes many technological systems, such as nuclear power plants, cannot be tested to destruction. Hence, uncertainties will always exist when trying to determine the maximum threshold of that particular technology. More common, of course, is the fact that prototype tests and routine quality assurance tests are sometimes carried out improperly. One notorious case involves the "fudging" of data by technical writers employed by B.F. Goodrich, which had a contract with the U.S. Air Force to design and produce a braking system for the A7-D aircraft (Vandivier, 1972). In short, one cannot uncritically trust testing procedures or those who manage and carry them out.

These categories of technical design failure are endemic to engineering design. Combinations of these factors were at the root of the collapse of the Dee Bridge, the Hyatt Regency walkway collapse, the Intel Pentium Chip crisis, and the Therac-25 computer failure.

In the Dee Bridge collapse, inadequate factors of safety, combined with extending a successful design beyond its load capacity through "fine-tuning" engineering, resulted in the collapse of the Dee Bridge at Chester, England, on May 21, 1887. The Dee Bridge, designed by Robert Stephenson and constructed in September 1846, collapsed due to torsional instability, indicating a major flaw in the new design. Five people were killed and 18 were injured as a locomotive and five carriages plunged into the river, destroying the bridge. According to Petroski, "The Dee Bridge failed because torsional instability was a failure mode safely ignored in shorter, stubbier girders whose tie rods exerted insufficient tension to induce the instability that would become prominent in longer, slenderer girders . . ." (Petroski, 1994: 95).

Petroski's analysis demonstrates that: "The critical flaw in the human design process that produced the ill-fated Dee Bridge is paradigmatic; the same fundamental flaw was rooted in the design process and environment that produced . . . a host of other doomed bridge designs" (1994: 83). Another example is the famous Tacoma Narrows Bridge, affectionately called "Galloping Gertie" because of its tendency to sway immensely when high crosswinds blew across the Narrows. Just months after its completion, the bridge came crashing down in September 1940. Countless bridges have collapsed because of design flaws. Petroski attributes these failures to what he terms the "success syndrome"; namely, the tendency for engineers to become overconfident by the past successes of a particular design in the process of extending it beyond the available fund of engineering knowledge and experience (1994: 83).

On July 17, 1981, the Hyatt Regency Hotel in Kansas City, Missouri, held a dance contest in its atrium lobby. The weight of the dancers and partygoers who populated the suspended walkways at the fourth and second floors proved to be more than the structures could withstand, causing the connections supporting the ceiling rods holding the second and fourth floor walkways to fail. Both walkways collapsed onto the crowded first-floor atrium. The ensuing investigation of the accident revealed a number of unsettling facts about the technical causes of the disaster and raised questions as to who should be held responsible for the loss of life and property.

During 1976, Crown Center Redevelopment Corporation (CCRC) began plans to design and build a Hyatt Regency Hotel in downtown Kansas City and hired GCE International (GCEI) as consulting structural engineers on the project. In 1978, Havens Steel Company was hired by CCRC to fabricate and install steel for the atrium lobby following GCEI's original design.

Hyatt Regency Walkway Collapse, July 17, 1981. Copyright AP/Wide World Photos. Used by permission.

The hotel consisted of a 40-story guest tower and a function block consisting of administrative offices and shops. Between these two structures was an atrium, which included three suspended walkways connecting the guest tower with the function block at the second, third, and fourth floors. The fourth floor walkway hung directly over the second floor walkway, which was connected to the fourth floor walkway with steel hanging rods. The third floor walkway hung separately from steel rods attached to the ceiling of the atrium. The original design developed by GCEI was to run a single support rod from the ceiling, through the fourth floor support box beams and right through the centerline of the second floor box beams. Finally, the steel rod would be attached at the bottom of the second floor beam with bolts and washers. As designed, the structural load from the box beam—the amount of weight the beam is supposed to support—would transfer to the supporting hanging rod. A washer and bolt on the rod below the beam would support the weight shift from the walkway beam supports to the steel hanging rods fastened to the ceiling.

In 1979, during a series of miscommunications between Havens Steel and GCEI, a design change was made in the fourth floor rod-beam connection from a single rod design to a two rod design. This change basically doubled the weight load placed on the bolt and washer set of the fourth floor connection, because instead of supporting just one box beam, as in the original design, it now had to support the weight of two box beams.

The official investigation determined that the modified design was the technical cause of the disaster. In particular, the report found that:

- The collapse initiated at the fourth-floor box-beam hanger-rod connection
- The as-constructed beam-rod connection did not meet Kansas City Building codes, nor did the original continuous rod design
- The change in rod design essentially doubled the transfer load from the beam through the nut to the steel hanging rod (Roddis, 1986: 1549–1550)

In other words, an improper design led to a structural failure that could have been avoided had the structural engineers who produced the original design examined carefully the design changes introduced by the steel fabricator.

The Missouri Board of Architects, Professional Engineers, and Land Surveyors brought civil charges against the engineers involved in the case, and a 27-week administrative law hearing ensued. The hearing board concluded that the design engineers for GCEI were fully responsible for the accident. It ruled that, in the preparation of their structural drawings, "depicting the box beam hanger-rod connection for the Hyatt atrium walkways, [GCE] . . . failed to conform to acceptable engineering practice. [This is based] upon evidence of a number of mistakes, errors, omissions and inadequacies contained on this section detail itself and of [GCE's] alleged failure to conform to the accepted custom and practice of engineering for proper communication of the engineer's design intent" (Anonymous [a], 1985).

The failure was ultimately caused by improper design changes that resulted in inattention to the impact of changes on the load forces acting on the connections while in operation. This case leads to questions concerning the responsibilities and obligations engineers have for the safe construction and implementation of their designs. After the hearing, the case was repeatedly discussed in the civil engineering community in professional journals and at academic conferences. Questions concerning the "legal costs of failure, professional liability, insurance, professional responsibility, project quality assurance, and professionalism in engineering" (Roddis, 1993: 1551) were discussed in the civil engineering community and resulted in a widespread examination of building codes and engineering practices. In particular, civil engineers learned from the disaster that "improved performance in the areas of detailing and connections, the recognition that structural detailing needs more attention in routine design and engineering education, and that structural schemes that lack redundancy demand an especially thorough design and careful review" (Roddis, 1993: 1551). These lessons should be heeded in order to avoid preventable technical design flaws in the future that could lead to disaster.

A major design flaw—more aptly designated as a technological failure rather than a technological disaster—is exemplified by Intel Corporation's Pentium computer chip. This case demonstrates that as designs become more complex, especially in the world of microprocessor and software design, tools and prototype testing become less capable of preventing and detecting design flaws (Betts, 1994: 4).

In November 1994, a mathematics professor disclosed on the Internet that Intel's new Pentium chip had a flaw that could lead to errors in some complex mathematical calculations. The flaw was discovered in the Pentium's FPU, or floating-point unit. The floating-point unit, generally implemented in computer hardware, is a method of calculation with varying numbers of decimal places. Floating-point units are used in spreadsheets, financial analysis software, graphics software, and scientific and engineering calculations. Intel had known of this flaw months earlier, but decided neither to announce the flaw to anyone nor to recall the defective chip. In retrospect, this decision was a costly public relations blunder, although, at the time, the decision was based on what top management at Intel considered to be plausible reasons. As Andrew Grove, former CEO of Intel, put it:

> We were already familiar with this problem, having encountered it several months earlier. It was due to a minor design error on the chip, which caused a rounding error in division once every nine billion times . . . [this meant] that an average spreadsheet user would run into the problem only once every 27,000 years of spreadsheet use. This is a long time, much longer than it would take for other types of problems . . . so, while we created and tested ways to correct the defect we went about our business. (Grove, 1996:12)

A week after customers began logging complaints on the Internet, Grove wisely decided to post an apology on the Internet. After a torrent of negative publicity based on these Internet exchanges, Intel offered to replace the defective chips for all customers, at a cost of $475 million to the company. As Andrew Grove eventually admitted:

> We basically defied our consumer population . . . We said 'we know what's good for them,' and we were pretty obstinate about that. In effect, we were ranking the consumers . . . we said, 'those of you that we decide merit a new chip will get a new one. The rest of you go away. You don't need one.' In retrospect, that was incredibly condescending and arrogant. (Grove, 1998: 117)

The $475 million that Intel took as a "write-off" consisted of estimates of the cost of replacement parts plus the value of the materials pulled off the line. According to Grove, the cost of replacement was the equivalent of half a year's R&D budget or five years' worth of the Pentium processor's advertising budget.

The flaw was the result of a design error that went undetected despite exhaustive design verification and testing. Such flaws are inevitable if microprocessor design engineers are pressured to dramatically increase quantity of output at the expense of quality of product. Contrary to the company's initial stance that mistakes with the FPU were limited to complex math only encountered by scientists, such calculation errors could conceivably affect business people designing currency trades, insurance contracts, and even computer-aided engineering design applications. Such flaws are often unacceptable in safety-critical applications.

Pentium's chip problem is simply one example of numerous product failures—both software as well as hardware—that have taken place in the computer industry. Peter G. Neumann (1995) has classified literally hundreds of computer-related risks causing millions of dollars of damage each year and causing potential safety hazards to scores of people. One hopes the Intel case will serve as a warning for the entire semiconductor industry (Williams, 1997).

According to Neumann, there have been a significant number of deaths due to computer-related failures. One such case involved the Therac-25 radiation device, designed to deliver doses of radiation to cancerous growths in patients in order to shrink their tumors. A flaw in the software that runs the device caused it to overradiate at least three patients, which ultimately lead to their deaths.

Between 1985 and 1987, the computer-controlled radiation linear accelerator, the Therac-25, gave massive overdoses of radiation to six patients—several of whom later died—at four different medical centers. The Therac-25 had a number of design flaws, including gaps in proper safety design, insufficient testing, and bugs in the software controlling the devices. In one case, a woman in Marietta, Georgia, received 20,000 rads (radiation absorbed dose) instead of 200 rads—100 times the intended dosage of radiation. The Therac-25 is equipped to deliver either electron beams (namely, "E-mode") or X-rays (namely, "X-mode"). In what has been described as a software programming error, the device had "scrambled" the "X-mode" and "E-mode" functions, delivering the deadly overdose (Jacky, 1990). Although original reports had attributed the failure to "operator error," it is now well recognized that the problem was caused by defects in the computer program and systems design that controlled the Therac-25 apparatus. One investigation of the Therac-25 disasters suggests that a partial cause of the problem is an organizational tendency of software development firms to not use proper software and safety engineering procedures; reliability testing procedures are notoriously absent even in the development of safety-critical systems such as medical devices (Leveson and Turner, 1993).

This case illustrates the problem of technical design factors in safety-critical systems, especially in the growing use of embedded microprocessors and microcomputers in the medical electronics industry. Researchers at the Federal Drug Administration report that almost all devices produced by the multi-billion dollar medical electronics industry now include embedded mini- or microchips. The Therac-25 case is one of the most serious computer-related failures to date (Joyce, 1987).

Henry Petroski, a profound student of engineering failures, develops a provocative assessment of engineering design successes and failures in his book *To Engineer is Human* (1985):

> [T]he colossal disasters that do occur are ultimately failures of design, but the lessons learned from those disasters can do more to advance engineering knowledge than all the successful machines and structures in the world. Indeed, failures appear to be inevitable in the wake of prolonged success, which encourages lower margins of safety. (p. xii)

Granted, many technological failures result from inadequacies in technical design. However, in looking for general principles that may elucidate the occurrence of technological disasters, we would nevertheless be unwise to restrict our attention to purely technical causes, for human, organizational, and sociocultural factors are also likely to be involved. The complexities created by such interrelationships are extremely important to examine as society continually tries to minimize the incidence of technological disasters.

Human Factors

The field of human-factors engineering deals with various cognitive, perceptual, and workplace design problems specific to technological systems operated by human beings, especially in the ever-increasing complexities of human-machine interfaces (Bignell and Fortune, 1984). Human factor causes of technological failures and disasters have led to the development of interdisciplinary fields such as industrial psychology and aviation psychology, which develop strategies for avoiding such systemic errors (Whetzel, 1997; Wiener, 1988).

Individual error is simply insufficient to account for the failure of increasingly complex and sophisticated technologies; hence the need to understand the structure of human-machine systems (Baron, 1990; Redmill, 1997). Of course, in some cases, the classic "pilot error" syndrome may account for some failures. "Pilot error," according to human-factors engineers, actually explains two categories of operator error. The first category of errors is referred to as *Type I.* Rochlin defines Type I errors as "overlooking, ignoring, or misunderstanding the information presented even when it occurs within the envelope of the predicted or anticipated flow of events" (1991: 114). Experts refer to the second category of error as *Type II.* Rochlin defines such errors as "accepting as true, accurate, or significant information that is misleading, incorrect, or irrelevant, or by extension, projecting into a situation 'external' beliefs or assumptions about the nature of the situation or state of the system" (Rochlin, 1991: 112; see also Landau and Stout, 1979). Both types of operator error seemed to be operating in the *Vincennes,* Three Mile Island, and Chernobyl cases. In the steamship collision involving the SS *Mendi,* we can identify Type I errors.

On the morning of February 21, 1917, the SS *Mendi* and the SS *Darro* collided 11 miles southwest of St. Catherine's Point on the Isle of Wight, causing 600 deaths out of 800 members of a native African labor battalion heading back to South Africa. The subsequent formal investigation into the high seas collision found the captain of the SS *Darro,* Henry Winchester Stump, guilty of failing to comply with articles 15 and 16 of the Regulations for Preventing Collisions at Sea, "as to sound signals and speed in a fog, and by its more serious default in failing, without reasonable cause, to send away a boat or boats to ascertain the extent of the damage to the SS *Mendi,* and to render her master, crew and passengers such assistance as was practicable and necessary, as required by section 422(1)(a) of the Merchant Shipping Act, 1894" (Clothier, 1987).

The accident at the Three Mile Island (TMI) nuclear power plant was a turning point for the nuclear power industry because it emphasized the central importance of human factors to safe plant operations. The President's Commission on the Accident at Three Mile Island stated that: "There are many examples in our report that indicate the lack of attention to the human factor in nuclear safety" (O'Hara, 1996: 46). The control room, through which the operations of the TMI plant were carried out, was lacking in many ways. The control panel was huge, including hundreds of alarm devices. Key indicator lights and switches were placed in locations where operators could not see them. The controls were described as "seriously deficient under accident conditions" (O'Hara, 1996: 46). One source of confusion during the crisis was the mismatch between what the computerized control mechanisms were communicating to the operators and their interpretation of the data. The operators interpreted the system as reporting that a crucial valve was closed when it was, in fact, left open for hours, allowing hundreds of gallons of coolant to pour out of the reactor core. Due to the myriad of human factors involved in the TMI accident, a Human Factors Evaluation Program Review Board was established in order to assist the Nuclear Regulatory Commission in conducting human-factors evaluations of the human-systems interfaces of advanced nuclear power plants (O'Hara, 1996).

As is well known from such reports, the causes of many technological disasters can be traced back to problems of cognitive processing of information, visual perception and its relation to visual displays (especially in information systems technologies), insufficiencies in human memory and retention, capacity for stress, cognitive and emotional overload, and operational burnout. These factors lead to bad judgment, inaccurate perceptions, and a host of other negative outcomes (Meshkati, 1992). It was such a set of factors that led to the shooting down of a civilian Iranian airliner by the USS *Vincennes*.

On the afternoon of July 3, 1988, during open battle with Iranian gunships, the USS *Vincennes* fired at and shot down a civilian Iranian Air jetliner, killing all 290 civilians aboard. The Hearing Board ruled that mistakes made in the interpretation of hyper-complex sociotechnical systems like the Navy's fully computerized AEGIS aircraft detection and warning system led to stress, "task-fixation," and unconscious distortion of data, all of which played a role in the *Vincennes* incident (Rochlin, 1991). As the findings reported, the AEGIS computer detection system initially misinterpreted the altitude of the Iranian Airbus, indicating it was descending, and initially identified the plane as an F-14 fighter jet. It eventually corrected itself, but it was reported that the crewmen monitoring the screens failed to detect the initial computer error.

Industrial psychologists call such events the "glass cockpit" syndrome, "a computer information overload in which the flood of technical information, faulty communications and outside stress lead to judgment errors" (Neumann, 1989: 7).

The Fogarty report on the USS *Vincennes* accident was unanimous in its recommendations:

> Since it appears that combat-induced stress on personnel may have played a significant role in the incident, it is recommended the CNO [Chief of Naval Operations] direct further study into the stress factors impacting on personnel in modern warships with highly sophisticated command, control, communications, and intelligence systems such as AEGIS. This study should also address the possibility of establishing a psychological profile for personnel who must function in this environment. (Rochlin, 1991: 107)

One can conclude that this case is an example of a human-machine mismatch. As one researcher put it, "the crew involved believed the initial system identification and altitude reading and did not double check them, nor did they change their evaluation when given new, conflicting information" (Neumann, 1989: 9).

The crucial role of human factors also surfaced in investigations into the Chernobyl nuclear disaster. During the early hours of April 26, 1986, Reactor 4 of the Chernobyl nuclear power plant exploded with two large blasts, releasing more than 140 million curies of radioactive material in a vapor cloud that eventually covered most of Eastern and Western Europe. Overall, 200,000 people were evacuated from 71 villages within an 18-mile radius of the plant.

Soviet experts carried out an exhaustive investigation of the disaster, using mathematical models and computer simulations to reconstruct the facts of the events. They presented their findings in a 430-page report, which they delivered to a meeting of the International Atomic Energy Agency (IAEA) held in Vienna, Austria, in August 1986. Their general conclusion was that the main cause of the accident was operator error. The Soviet report claimed that operator error led to "violations of the established order in the preparation of tests," "violation of the testing program itself," and "inadequate understanding on the part of the personnel of the operating processes in a nuclear reactor" (Serrill, 1986). The report also concluded that workers, operating with a sense of overconfidence, exhibited a "loss of a sense of danger" in managing the complex safety systems of the reactor (Serrill, 1986). Andronik M. Petrosyants, chairman of the Soviet Committee for the Peaceful Uses of Atomic Energy, echoed these findings when he stated that "the accident took place as a result of a whole series of gross violations of operating regulations by the workers . . . The sequence of such human actions was so unlikely . . . that the [design] engineers did not include such a scenario in [their] projects" (Serrill, 1986: 27).

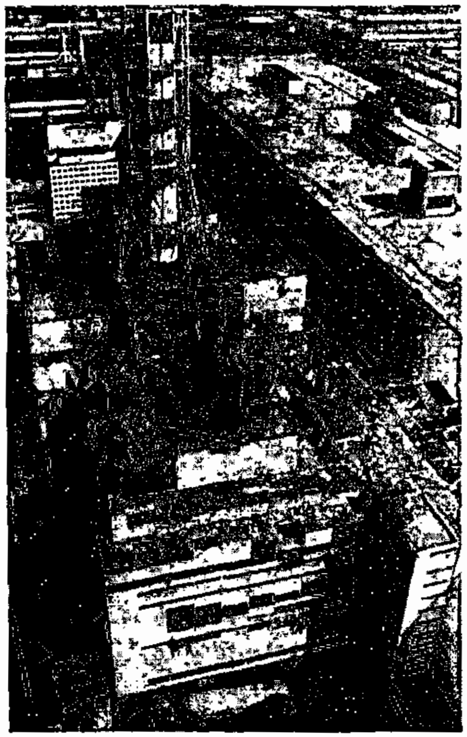
Although initially skeptical of the Soviet report, nuclear scientists tended to agree with the unprecedented candor of the Soviets. The conclusions of the report concerning operator error were echoed in various subsequent International Atomic Energy Agency (IAEA) reports. "The root cause of the Chernobyl accident it is concluded is to be found in the so-called human element. . . . The lessons drawn from the Chernobyl accident are valuable for all reactor types" (IAEA, 1986: 76). Or consider the following statement: "The Chernobyl accident illustrated the critical contribution of the human factor in nuclear safety" (IAEA, 1987: 43). Finally, in the words of Valery Legasov, Soviet delegate to IAEA: "I advocate the respect for human engineering and sound man-machine interaction" (Meshkati, 1991: 148). According to the report, operators at the plant committed six major errors, all of which led to one of the worst technological disasters in history.

On April 25, 1986, a test was being conducted on Reactor 4 of the Chernobyl plant in order to determine how long the turbines would continue rotating when cut off from the steam supply. This information was needed to ascertain how much energy would be generated from the mechanical inertia of the spinning turbines and, hence, for how long this rotation could run the generators if the plant was accidentally cut off from the power grid. The test was scheduled for a routine shutdown of the plant when power output was virtually discontinued, even though the reaction process continued to operate. This was the only time the test could be conducted, so operations management was anxious to have it done since it would mean waiting a full year if it was not. The plant operators began reducing the reactor's power output levels so they could run the turbine test.

To prevent the core from being flooded with excess water that would halt the test, the operators switched off the emergency backup cooling system. They proceeded to bring the power output down to between 700 and 1,000 megawatts (thermal) and then cut off steam to one of the turbines. At this time, an order came in from a grid manager at Kiev, who asked the Chernobyl power plant to maintain the power output at normal levels to service requests for power from the local community. Therefore, the test had to be postponed until 11:00 p.m. that evening.

The *first* of six major human factors errors occurred when, violating safety rules, the operators failed to switch the emergency cooling system back on. The test resumed at 11:10 p.m. and control was transferred from a local to an automatic regulating system. Committing their *second* major error, the operators did not set the automatic system above the minimum output level of 700 MW(t). This was a serious omission because the reactor had a tendency to become unstable at low output levels. This caused the reactor output level to drop quickly to around 30 MW(t). Reducing the power output to this low level caused the nuclear fission reaction to slow down, causing poisonous xenon gas buildup in the fuel rods. Xenon gas absorbs electrons and slows down the fission process, thus decreasing overall energy output.

The operators had available a variety of manual controls with which to increase the power output levels. By withdrawing all but eight or ten of the control rods, violating safety regulations which required at least 30 control rods to be plunged into the reactor at all times, they managed to bring the power up to 200 MW(t). This resulted in their *third* major mistake. In hindsight, given the difficulty of maintaining stability in the core, the best thing the operators could have done at this point was to either bring the test to a halt, or postpone it until the xenon gas had decayed. Instead, the operators only compounded their earlier blunders with reckless attempts to force the output level to increase power. To accomplish this they switched on additional pumps in order to increase the water flow to the core. However, because the reactor was running at lower power than originally planned, too much cooling water flowed through the core, which in turn caused the steam pressure and the water level in the steam separators to drop. In order to prevent the reactor from shutting down automatically when these parameters fell below the critical point, the operators blocked signals from pressure and water sensors, thereby disabling a key part of the emergency shutdown system. This constituted their *fourth* major violation of safety procedures.



Chernobyl Nuclear Catastrophe, April 25, 1986. Copyright Getty Images, Inc. Used by permission.

The decrease in steam generation caused by the excess cooling water prompted the automatic control rods to be withdrawn completely. The operators then withdrew virtually all of the manual rods in order to maintain the power level at 200 MW(t). This further reduced the operating margin and the capacity to respond quickly in an emergency. In what constituted their *fifth* major error, operators switched off a second defense mechanism, which would shut down the reactor in the event that steam levels in the steam separator fell below normal. Nevertheless, the reactor appeared to be stabilized and, at 1:23 a.m., the steam supply to the generator was shut off, thus finally initiating the actual test. The flow of water into the reactor was decreased radically as four of the main circulation pumps and the two main pumps feeding water into the reactor were disengaged. The sudden decrease in water caused the temperature to rise, greatly increasing the amount of steam being generated. This was their *sixth* and final error (Sweet, 1989).

The reactor was operating at low power, a state in which a small increase in power causes a larger increase in steam, which in turn causes an unexpected increase in power. Boiling increased and, because of the positive void coefficient, the power started to climb sharply. At 1:23 a.m. the shift manager gave the order to hit the emergency button, which plunged the control rods into the reactor to stop the nuclear reaction. However, because the rods were almost completely withdrawn, the response time was too slow.

By this time, the situation was out of control. Intense steam generation was taking place around the fuel elements, which in turn reduced the system's heat removal ability. The power output continued to surge and the fuel started to disintegrate and fall into the cooling water. The result was a sharp increase in pressure, which ruptured the cooling channels and prompted a thermal explosion that destroyed the reactor and part of the structural components of the building. This ruptured some of the pressure tubes passing through the massive graphite moderator and circulating water around the fuel rods. Without cooling water, the fuel elements rapidly heated up and began to melt. Experts theorize that a highly combustible mixture of gases such as hydrogen and carbon monoxide was formed when steam came into contact with the hot graphite that, combined with the zirconium in the fuel rods, reacted with the superheated steam to produce even more hydrogen.

Within a few seconds, a mighty surge erupted, from 200 to 32,000 MW(t) or 100 times full power. This was followed immediately by a further surge of power to about 440 times normal level. The result was catastrophic.

Here we witness the complex interactions of the human-machine interface. The failure at Chernobyl demonstrates the complex interaction between human factors and technical design factors. In addition to the human factors discussed previously, three principal design defects of the RMBK-1000 (Russian Graphite-Moderated Reactor) are:

1. The fact that the reactor tends to gain power rather than slow down as water is lost or is turned to steam. This makes the reactor highly unstable when there is low power output.

2. Inadequate containment surrounds the reactor core.
3. The design of the system does not provide or protect against operator interference with the safety systems (Norman, 1986).

The Chernobyl case involves a combination of human factors and technical design factors that resulted in a catastrophe.

After 14 years of pondering this disaster, the Ukrainian government, in cooperation with a group of seven industrial nations, signed a formal agreement to shut down the Chernobyl power plant by the year 2000. In signing the agreement, the European Union and the United States agreed to help Ukraine devise plans to mitigate the effects of the shutdown on local populations (Shcherbak, 1996). This agreement has come to fruition. The Chernobyl plant was finally shut down on December 15, 2000 (Sciolino and Gordon, 2000: 1).

We now turn to the third root category of technological failure: organizational systems factors.

Organizational Systems Factors

The organizational contexts in which technological systems operate add to their complexity and susceptibility to failure in at least three ways. First, organizational strategies, policies, and financial and human resources determine the level of attention devoted to managing technological systems and therefore dictate how technological systems are operated. Thus, the nature and the culture of the organization establish the level of reliability and safety at which a technology is operated. Second, the vagaries in communication and decision making in large organizations are aspects of corporate culture that are especially vulnerable to faulty group decision making and often lead to organizational failure. Many researchers have examined the complexities of corporate communication and group decision making, focusing on inadequate procedures that may eventually lead to breakdown and failure of technological systems (e.g., see Janis, 1972; Fisher, 1986; Baskin and Aronoff, 1988; Corman *et al.*, 1990). Third, organizational failures in the form of inadequate attention to safety create preconditions for failure in corporations that are involved with high-risk technologies.

Organizational systems factors were at work in the sinking of the *Sultana.* On April 27, 1865, as the Civil War was ending, the greatest marine disaster in the history of the United States occurred on the Mississippi River, a few miles above Memphis, Tennessee, when the boilers on the steamship *Sultana* exploded and burned, killing at least 1,250 passengers and crew. The *Sultana* was a packet side-wheeler: 260 feet long, 42 feet wide, displacing 719 tons of water, with a cargo capacity of 1,300 tons and licensed to carry 376 passengers. Two steam engines drove the side wheels. The steam was provided by four tubular boilers that were, at the time, an experimental design. While docked at Vicksburg, Virginia, the captain was alleged to have taken bribes to allow more than 1,800 men, former prisoners of war, to be loaded onto the boat. That fateful day, the *Sultana*'s boilers were pressured beyond capacity due to the excess weight of the passengers. The boilers suddenly burst with a terrific explosion. In the opinion of Inspector Witzig and P.B. Stillman, President of the Steamboat Inspection Board, the cause of the disaster was laxity in the enforcement of safety regulations during the war that had produced a climate of "carelessness, recklessness, and poor judgments" which made steamboat travel on the Mississippi dangerous (Salecker, 1986; Yager, 1976).

Violations of government safety regulations, compounded by pressures to conform to policies of large private corporations, are frequent causes of technological disasters. This is exemplified in the B.F. Goodrich brake scandal. In August 1969, Kermit Vandivier, a data analyst and technical writer for B.F. Goodrich, testified before Senator William Proxmire's Economy in Government Subcommittee hearing that he was part of a conspiracy to commit fraud and deception in an alleged cover-up that included lying to the U.S. Air Force and fudging technical data to make an unsafe brake system appear safe (Vandivier, 1972). It all began when B.F. Goodrich secured a contract with LTV Aerospace Technologies to supply 202 braking assemblies, which would be installed in a new attack plane, the A7D.

B.F. Goodrich had fallen out of grace with LTV, and had not received any offers from them in years. Contracts to build brake systems for military aircraft are generally lucrative, so when an offer finally came to Goodrich in June 1967, top managers decided they must secure the contract at all costs, and, bidding outrageously low, Goodrich received the contract to build the braking systems for the A7D. John Warren, a seasoned design engineer and one of Goodrich's best design engineers, was named project engineer and went to work. In a relatively brief time Warren produced a preliminary four-pad design. After several unsuccessful tests, Searle Lawson, a newcomer at Goodrich, arrived at the conclusion that the brake design was fundamentally flawed. During every trial, the brake became very hot, sometimes glowing red and radiating "incandescent particles of metal and lining." After these trial runs, the brake lining had disintegrated and turned to dust.

After extensive testing, Lawson concluded that the brake was too small. The four-disc design was inadequate, and a five-disc brake design was needed. Lawson reported his findings and concerns about the flawed design to his boss, John Warren. Warren rejected the suggestion that the brake was too small and simply requested that Lawson return to the prototype testing. Unconvinced, Lawson went to an engineering project supervisor, Robert Sink, who dismissed the claim that Warren's design could be faulty but seemed to be concerned about the data the tests were generating.

On the 13th test, Vandivier became involved when he was given the rask of putting together the test data for the A7D and creating a qualification report. In reviewing the data, Vandivier discovered an irregularity. It seemed as if the recording instrument used to calibrate brake pressure had been deliberately miscalibrated to make it seem that less pressure was required to stop the aircraft than was the case.

Vandivier immediately showed the miscalibrated test logs to his lab supervisor, Ralph Gretzinger, who was aware of the deliberate data tampering, because he heard that Lawson had ordered the miscalibration on instructions from Robert Sink. Both men vowed not to have anything to do with the intentional "cooking" of the data. In a discussion between Vandivier, Gretzinger, and Lawson, Lawson said he was told, "regardless of what the brake does on the test, it's going to be qualified" (Vandivier, 1972: 214). Angered, Gretzinger went directly to Russell Line, who was responsible for engineering lab testing. Gretzinger returned, greatly saddened by his conversation with Line. He confided to Vandivier and Lawson, "I've been an engineer for a long time, and I've always believed that ethics and integrity were every bit as important as theorems and formula . . . Now this . . . Hell, I've got two sons I've got to put through school. . . ." As Vandivier put it: "He [Gretzinger] had been beaten down. He had reached the point where the decision had to be made. Defy them now while there is still time or knuckle under, sell out" (Vandivier, 1972: 215).

These men found themselves impaled on the horns of a dilemma: write the deceptive report and save their jobs at the expense of their consciences, or refuse to write the report, thus honoring their moral beliefs but risking being fired. Vandivier called Lawson and told him he would write the report as requested, directed from "upstairs" to "fix" the data.

> Lawson and I proceeded to prepare page after page of elaborate, detailed engineering curves, charts, and test logs, which purported to show what had happened during the formal qualification tests. When temperatures were too high, we deliberately chopped them down a few hundred degrees, and where they were too low, we raised them to a value that would appear reasonable to the LTV and military engineers—everything of consequence was tailored to fit the occasion. Occasionally, we would find that some test or other either hadn't been performed at all or had been conducted improperly. On those occasions, we 'conducted' the test—successfully, of course—on paper. (Vandivier, 1972)

In June 1968, the report was completed and sent to all concerned parties. Vandivier, Lawson, and Warren refused to sign the report, but, soon after, test flights commenced. Test flights led to several near crashes on landings, the brakes even welding together during one test, causing the plane to skid for over 1,500 feet. It was at this point that Vandivier's lawyer advised him to go to the authorities, and he told everything to the Federal Bureau of Investigation (FBI). The FBI tipped off the Air Force and they stopped all testing and demanded from Goodrich all raw data compiled on the prototype testing. Vandivier handed in his letter of resignation, and in the letter he stated:

> As you are aware, this report contained numerous, deliberate, and willful misrepresentations which, according to legal counsel, constitutes fraud and exposes both myself and others to criminal charges or conspiracy to defraud. The events of the past seven months have created an atmosphere of deceit and distrust in which it is impossible to work. (Vandivier, 1972)

Vandivier left the company and became a newspaper reporter for the *Daily News* in Troy, Ohio. At the Senate hearings, lawyers for B.F. Goodrich portrayed Lawson as too young and inexperienced and denigrated Vandivier for his "lack of technical training," which was confirmed by Sink, who represented B.F. Goodrich at the hearings. Within only four hours, the committee adjourned, making no recommendations and finding no one guilty. Lawson stayed on the A7D project; Line was promoted to production superintendent and Sink moved into Line's old job.

The A7D brake scandal is a particularly valuable case because it provides insight into group dynamics and the mechanisms leading to corporate deviance (see Chapter 11). In this case, top engineers committed to a course of actions and capitulating to managerial pressures endangered human lives. Given that senior engineers were prepared to falsify data, it is difficult to conceive of watertight testing procedures that are not amenable to manipulation if people are really intent on falsifying technical documents.

Another case study demonstrating the importance of whistle blowing (see also Chapter 11) is the case of the three engineers involved in the construction and testing of the Bay Area Rapid Transit (BART) system. In September 1972, the San Francisco BART system began operations. The system was hailed as the nation's first space-age, completely automated transit system. Less than a month after its first run, on October 2, a train failed to stop at one of the stations, shot off the track, and crashed into a nearby commuter parking lot. BART management downplayed the incident, as well as other malfunctions that plagued the system, as a process of "getting the bugs out." Other problems included doors suddenly opening as trains raced down the track, trains speeding through stations when programmed to stop, brake controls malfunctioning and detection of "phantom trains" causing real trains to stop. In an anonymous memo to the BART Board of Directors, three engineers alleged that the automatic train control system was unsafely designed, that testing and operator training were inadequate, that there were excessive cost overruns, and that computer software problems plagued the system (Anderson *et al.*, 1980). On March 2, 1972, the three engineers were fired.

Another prominent case of technological disaster, the Challenger explosion, is attributable to the negative effects of the hierarchical structure of corporations, the vagaries of communication in large organizations, and the impact of corporate culture on decision making. The Challenger space shuttle 51-L exploded on January 28, 1986, 73 seconds after liftoff, killing its crew of seven, including the first potential civilian in space. In addition to the tragic loss of life, $55 million of taxpayer dollars went up in smoke along with the shuttle and rocket. There is a growing amount of literature discussing the various organizational and communication factors that led to this disaster, each researcher stressing different facets of the precipitating organizational and communicative breakdowns (Hirokawa, 1988; Gouran *et al.*, 1986; Herndl, 1994; Dombrowski, 1992; Winsor, 1990; Moore, 1992; Pace, 1988; Miller, 1993; Rowland, 1986; Renz and Greg, 1988).

The Challenger case demonstrates unequivocally that flawed decision making—arising from complex interactions between engineers and managers with different objectives in the hierarchies of NASA and its contractor, Morton Thiokol—is one of the primary causes of technological disaster. In a much discussed three-way teleconference the night before the launch, engineers from Morton Thiokol sought to persuade NASA and Morton Thiokol management to abort the launch. At that point Jerry Mason, senior vice president of Morton Thiokol, turned to Robert Lund, vice president of engineering at Morton Thiokol, and asked him to "take off his engineering hat, and put on his management hat." In complying with this request, Lund rejected the no-launch recommendation of his engineers and made the decision to proceed with the launch. In addition, miscommunication, fostered by diverse corporate cultures that emphasize compliance with rules and regulations, created a great deal of stress. When one superimposes unquestioning obedience to the chain of command, we have the precondition for the occurrence of a technological disaster.

In a nine-year study of the Challenger case, Diane Vaughn presents an elaborate analysis of the corporate cultures of NASA and Morton Thiokol, in which she interprets the acceptance of risk by Morton Thiokol and NASA engineers, in spite of growing evidence of O-ring erosion problems, as a "normalization of deviance."

> The two engineering communities . . . came to the same conclusion: the design, although deviating from performance expectations, was an acceptable risk. . . . These two early conclusions—accept the risk and proceed with flight; correct rather than redesign—would become norms guiding subsequent decision-making, characterizing the work group culture in the years to come . . . . (Vaughn, 1996: 106)

In her concluding chapter, "Lessons Learned," Vaughn interprets the Challenger disaster as an example of Perrow's Normal Accident Theory: "an organizational-technical system failure that was the inevitable product of the two complex systems" (Vaughn, 1996: 415).

As the foregoing discussion of various cases has demonstrated, technical, human, and organizational factors cause many technological disasters and, consequently, have been studied extensively. Nevertheless, these three categories do not exhaust the causes of technological disaster. Crisis management theorists label these "internal" factors (Shrivastava, *et al.*, 1998). As explanatory as these three factors may be, they do not include "external" factors. Since the latter also generate technological hazards, their analysis is essential to understanding technological disasters. To our view, no theory of hazard management and technological disaster is complete without understanding *both* internal and external forces. Much of the literature does analyze external factors (economic, political, social, and cultural); however, it restricts the analysis to factors internal to organizational systems. The societal context of technological disasters must also be studied, analyzed, and understood. We now turn to these external factors.

Socio-Cultural Factors

Socio-cultural factors combine sociological and anthropological concepts of social structure and culture. Social structure refers to social institutions such as economic, political, legal, familial, religious, and educational organizations. Culture refers to the system of norms and values governing the behavior of members of a society. Economic, legal, and political institutions can either deter or promote the occurrence of technological disasters. Cultural factors include the values placed on safety and human life, attitudes towards risk—risk-aversive behavior vs. risk-taking behavior—as well as the individual's autonomy vs. his or her responsibility toward the group.

On December 6, 1907, 366 coal miners lost their lives in one of the worst coal mine disasters in U.S. history when a runaway cable car smashed into electric cable lines in a mine outside of Monongah, West Virginia (Jackson, 1982). In addition to the Monongah disaster, several other major mine explosions occurred in 1907. The resulting public outcry and grief demanded governmental intervention. This led directly to the establishment of the Bureau of Mines, which was the culmination of the U.S. government's growing involvement in the mining industry. The mine disasters of 1907 laid a capstone on a deteriorating situation. Between 1906 and 1908, a total of 22,840 coal miners had been killed in the United States alone; the number of fatal accidents had nearly doubled in the preceding six years. In 1907, 3,200 miners were killed, one-half in Pennsylvania. The frightening carnage was blamed on the lack of reliable information concerning the safety of explosives and the lack of enforceable mine regulations (Jackson, 1982).

On March 25, 1911, a fatal conflagration occurred in a sweatshop, The Triangle Shirtwaist Factory, which resulted, eventually, in a national movement for safer working conditions in the United States (Stein, 1962). The fire started on the eighth floor of the Asch building in lower Manhattan. One hundred and forty-six workers died, mostly young women, many of them as young as 14 years old. Like most other sweatshops, the Asch building had no sprinkler system, its doors opened inward, it had two staircases rather than the required three, and the fire escape exit led only to the roof. Some workers, having no way of opening the doors that had been locked to prevent employee theft, leapt to their deaths from seventh and eighth story windows.

The American poet laureate Robert Pinsky captures the poignancy of this tragedy in his poem "Shirt" (Pinsky, 1990).

> . . . At the Triangle Factory in nineteen-eleven.
> One hundred and forty-six died in the flames
> On the ninth floor, no hydrants, no fire escapes—
>
> The witness in a building across the street
> Who watched how a young man helped a girl to step
> Up to the windowsill, then held her out
>
> Away from the masonry wall and let her drop.
> And then another. As if he were helping them up
> To enter a streetcar, and not eternity.

A third before he dropped her put her arms
Around his neck and kissed him. Then he held
Her into space, and dropped her. Almost at once

He stepped up to the sill himself, his jacket flared
And fluttered up from his shirt as he came down,
Air filling up the legs of his gray trousers . . .

The disaster led to the creation of health and safety legislation, including factory fire codes and child labor laws, and helped shape future labor laws.

In December 1991, a San Francisco court found Dow Corning guilty of manufacturing a dubiously safe product, namely, its line of breast implants. The plaintiff, Mariann Hopkins, was awarded $7.3 million, $840,000 in compensatory damages and $6.5 million in punitive damages. This caused a wave of silicon-implant litigation, and, by 1993, the Food and Drug Administration (FDA) had received an estimated 3,000 reports of illnesses or injuries associated with silicon implants, which had been implanted in more than 1 million women. Women claiming sickness and disease from the implants filed more than 1,000 lawsuits. In 1993, a Texas state court awarded $25 million to a claimant against the Bristol-Meyers Squibb Corporation. Among the many health problems alleged to have been caused by silicon implants are: autoimmune diseases such as lupus, arthritis, scleroderma, breast cancer, abnormal tissue-growth, nerve damage, inflammations, swollen joints, rashes, and fatigue.

In the Hopkins case, the jury found Dow Corning guilty of fraud after having obtained access to reams of company memos that showed numerous complaints by company researchers and management about the implants. These complaints included ruptures, leakages, infections, and autoimmune system problems. During the trial, Thomas Talcott, a former Dow Corning materials engineer who conducted silicon breast implant research testified that, "The manufacturers and surgeons have been performing experimental surgery on humans" (Hartley, 1993). In 1992 Dr. Sydney Wolfe, director of the Public Citizen Health Research Group, accused Dow Corning of actively covering up important information concerning health risks associated with silicon breast implants.

> They [Dow Corning Corporation (DCC)] are reckless and they have a reckless attitude about women. . . . DCC was only thinking of themselves when they repeatedly assured women and their doctors that the implants were safe . . . [keeping] guard over hundreds of internal memos that suggested that some of Dow Corning's employees have long been dissatisfied with the scientific data on the implants. (Hartley, 1993)

These unsettling facts raise the issue of why the silicon implant devices were not more closely regulated by the FDA. A brief recounting of the role of the FDA in the history of the breast implant controversy will shed light on socio-cultural factors, such as regulatory and other institutional mechanisms that often fail in their roles to manage and control new and/or potentially risky technologies. If adequate regulation is not effective, the potential for technological disasters increases.

In 1976, Congress passed the Medical Device Amendment to the Federal Food, Drug, and Cosmetic Act of 1938, placing, for the first time, medical devices such as silicon breast implants under regulatory scrutiny. This amendment was motivated largely by the Dalkon Shield catastrophe. Among other things, the 1976 amendment directed the FDA to set up an approval process for new devices and classify existing ones into Class I, II, or III, depending on the degree of testing necessary to provide reasonable proof of the safety of the device (see Chapter 11 for a further discussion).

A preliminary review was carried out by the FDA's General and Plastic Surgery Devices Advisory Panel, a group dominated by plastic surgeons. This review placed silicon breast implants in the less restrictive Class II category, which required minimal review and did not even require testing for the product to remain on the market. No further inquiries into breast implants were made until a growing list of consumer and scientific complaints forced the FDA to look into the safety and efficacy of the implants. Finally, in early 1989, the FDA acknowledged silicon breast implants to be Class III devices and required all implant manufacturers to produce detailed information and scientific research about the implants' safety and reliability. In 1991, satisfied with the information, the FDA ruled to allow all manufacturers, including Dow Corning, to continue to manufacture, market, and sell silicon breast implants without further research.

At the same time, though, concern was growing among research physicians and consumer groups about the overall safety of the implants. A growing number of FDA scientists disputed the initial findings based on feedback from physicians, who reported numerous cases of leaking or ruptured implants. In 1992, David Kessler, FDA commissioner, announced a 45-day moratorium on the sale of silicon breast implants. Until recently, the FDA had placed a total ban on breast implants, save for legitimate circumstances of reconstructive surgery.

The Institute of Medicine (IOM) published its review of all scientific research on breast implant safety in early 2000 (Bondurant, Ernster, and Herdman, 2000). The IOM report concluded that silicon breast implants could pose enough localized complications that their safe use could be compromised. The IOM report stated that deflation, rupture, and leakage can indeed occur. Other localized complications identified were injury, pain, infection, hematoma, necrosis, and tissue atrophy, among other complications. Finally, the IOM report, the most authoritative and up-to-date of its kind, recommended that the use of silicon breast implants be limited to persons eligible for reconstruction after breast cancer surgery. One reason the report gave for limiting implants to augmentation patients is that the risks outweighed the benefits of the surgery for patients seeking breast enhancement.

Even more recent than the IOM report is a study in 2001 by researchers at the National Cancer Institute demonstrating that women with breast implants "suffer higher rates of lung and brain cancer than other plastic surgery patients" (Stolberg, 2001: A19).

The socio-cultural factors operative in this case include the ever-changing cultural standards of feminine beauty. As regards breast implants, one influential group, the American Society for Plastic and Reconstructive Surgery (ASPRS), a professional association representing 97 percent of all board-certified plastic surgeons, lobbied hard to redefine female flat-chestedness as a medical disease requiring medical treatment. In July 1982, the ASPRS filed a formal recommendation to the FDA arguing that:

> There is a substantial and enlarging body of medical opinion to the effect that these deformities [small breasts] are really a disease, which in most patients results in feelings of inadequacy, lack of self-confidence, distortion of body image and a total lack of well-being due to a lack of self-perceived femininity. The enlargement of the underdeveloped female breast is, therefore, often very necessary to insure an improved quality of life for the patient. (Lawrence, 1993: 245)

It seems fair to remark that the ASPRS is at least partly responsible for the rush to manufacture and market silicon breast implants without the benefit of appropriate scientific research and development.

The current social pressures to conform to cultural standards of feminine beauty are summed up in a special 100th anniversary edition of *Vogue* magazine, published in 1992. The magazine states:

> . . . And in women's bodies, the fashion now is a combination of hard, muscular stomach and shapely breasts. Increasingly, women are willing to regard their bodies as photographic images, unpublishable until retouched and perfected at the hands of a surgeon. (Lawrence, 1993: 247)

The three foregoing cases—the mine disaster in Monongah, the Triangle Shirtwaist Factory fire, and the Dow Corning silicon implant injuries—underscore the impact of social structure and culture on technology as it affects our lives. Without effective regulation to protect employees and consumers, some corporate enterprises operate with a bottom-line focus to the detriment of the lives of consumers affected by their products and operations.

Socio-cultural systems factors contributing to technological disaster are important because they identify failures that have causes external to organizations, involving social, political, and cultural variables. Hence, technological disasters cannot be understood simply as design failures, operator failures, or organizational failures. In other words, the prevention and management of technological disasters cannot be achieved at the organizational level alone. The harder task is effecting changes in the institutions and the culture of a society, and strategies must be developed to promote more effective societal control of technologies.

The four root causes underlying technological disaster, together with their associated elements, are summarized in Figure 5–2.

Technical Design Factors	Human Factors
• Faulty design • Defective equipment • Contaminated or defective materials • Contaminated or defective supplies • Faulty testing procedures	• Human-machine mismatches • Operator error • Perceptual constraints • Fatigue or stress • Ignorance, hubris, or folly
Organizational Systems Factors	Socio-Cultural Factors
• Communication faulures • Faulty group decision making • Policy failures • Cost pressures curtailing attention to safety	• Cultural values and norms • Institutional mechanisms Regulatory mechanisms Educational systems

Figure 5-2
A classification of causes of technological disasters.

Terrorism in the Nuclear-Information Age

In reviewing our four categories of causes of technological disasters we have not attended to terrorism as a menace intrinsic to the technologies of our age. Fortunately, terrorists have not yet applied their criminal designs to potentially vulnerable technologies such as nuclear power plants. According to Dumas, however, there is little comfort in this observation.

> [T]here is nothing inherent in the nature of terrorism that makes it self-limiting. Those who are ready, even eager, to die for their cause, who stand willing to abandon every constraint of civilized behavior and moral decency against the slaughter of innocents, cannot be expected to permanently observe some artificial restriction on the amount of havoc they wreak. (Dumas, 1999: 56)

Events in recent years attest to this dismaying fact.

For many years, the United States Government has been required, by statute, to publish annual country reports on terrorism. The statutory definition of terrorism is as follows: "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents" (U.S. Code Title 22, section 2656f [d]). Pillar has cogently explicated four principal elements in this definition: (1) "premeditation, means there must be an intent and prior decision to act that would qualify as terrorism;" (2) "political motivation, excludes political violence motivated by monetary gain or personal vengeance;" (3) "that the targets are noncombatants, means that terrorists attack people who cannot defend themselves with violence in return;" and (4) "that the perpetrators are either subnational groups or clandestine agents, is another difference between terrorism and normal military operations" (Pillar, 2001: 13–14).

Some legal scholars have pointed to the need for a general definition of terrorism that would cover both state-sponsored terrorism as well as terrorism by non-state actors. The increasing occurrence of threats of highjacking, bio-chemical terrorism, and nuclear terrorism may produce a steady growth of international treaties addressing such acts. "What is needed at this juncture is the establishment of a global legal regime dealing specifically with terrorism" (Mendlovitz, 2001: 3).

Terrorist attacks have been more common in the last few decades than we would like to think. According to statistics from the U.S. Department of State, there were approximately 13,000 incidents of terrorist attacks from 1968 through 1997, or "an average of more than 430 per year for three decades" (Dumas, 1999: 55).

In the 1980s, a wave of hijackings and bombings targeted the airlines, especially foreign carriers flying without the stringent security measures imposed by the FAA on U.S. airlines. "This isn't just a matter of economics but security may be a primary reason why foreign carriers have been successfully sabotaged far more often than U.S. airlines" (Nader and Smith, 1993: 294). Table 5-1 presents a list of explosions on aircraft between 1980 and 1989. These grim statistics provide a compelling argument for developing uniform international security measures governing airlines such as those El Al airlines has implemented over the years. "Israel's El Al airline spends 8% of its revenue on security, 75% of which is subsidized by the government. American airlines, by contrast, pay only 0.2%-0.3% of their revenue toward security" (Lopez, 2001: 1).

In the 1990s, two enormously destructive terrorist bombings occurred. On February 26, 1993, Mohamed Salemeh and Ramzi Yousef, two alleged terrorists, placed a bomb in a van driven into

Table 5-1
Explosions on aircraft between 1980 and 1989.

Year	Airline	Location	Circumstances	Casualties
1980	United (USA)	Sacramento	Explosion in cargo hold while plane being unloaded	2 injured
1981	Air Malta (Malta)	Cairo	2 bombs explode as luggage being unloaded	2 killed 8 injured
1982	Pan American World Airways (USA)	In flight near Hawaii	Bomb under seat cushion exploded	1 killed 15 injured
1983	Gulf Air (Bahrain)	In flight	Bomb exploded in baggage compartment	112 killed
1984	Union Des Transport (France)	Chad	Bomb exploded in cargo hold after landing	24 injured
1985	Air India	In flight	Bomb exploded in cargo hold	329 killed
1986	TWA (USA)	In flight	Bomb exploded in cabin over Greece	4 killed 9 injured
1987	Korea Airlines	In flight	Bomb in cabin area	115 killed
1988	Pan Am 103	In flight	Bomb in cargo area	270 killed
1989	UTA	In flight	Mid-air explosion	171 killed
1989	Avianca (Columbia)	In flight	Bomb under seat	107 killed

Source: Data compiled by the President's Commission on Aviation and Security; reproduced in Ralph Nader and Wesley J. Smith (1993). *Collision Course: The Truth about Aviation Safety.* Blue Ridge Summit, PA, pp. 294–295.

the basement of the World Trade Center in New York. The eventual explosion killed six people and injured more than 1,000 (Farley, 1995). On April 19, 1995, Timothy McVeigh blew up the Alfred P. Murrah Federal Building in Oklahoma City, killing 168 people (Witkin and Roebuck, 1998; Yardley, 2000).

In 1996, an intellectual Luddite by the name of Theodore Kaczynski, otherwise known as the "Unabomber," was arrested. The author of an anti-technology "manifesto" entitled "Industrial Society and its Future" (Kaczynski, 1995), Kaczynski was determined to stop the drift of civilization to self-destruction by launching a campaign of terror. It began on May 26, 1978, when his first bomb slightly injured a Northwestern University safety officer, and ended on April 24, 1995, when a bomb he mailed killed the president of the California Forestry Association. Altogether, he mailed

or delivered sixteen package bombs to scientists, academics, and others over a period of 17 years, killing 3 people and injuring 23. Kaczynski pleaded guilty to all of his crimes and was sentenced to life in prison without the possibility of parole (Chase, 2000).

When Americans think of the form a conventional terrorist attack might take, they probably think of hijackings like those that occurred during the 1980s, or bombings like the ones perpetrated by Salameh and Yousef and Timothy McVeigh, or assassinations such as those committed by Kaczynski. These are not the only forms of terrorism, however. Terrorists have begun to exploit the vulnerabilities of information technologies such as the Internet. The use of information technology to terrorize is called cyberterrorism. Cyberterrorism takes many forms, including infecting computer networks with deadly computer viruses that sabotage and delete information and erase computer files, or distributed denial-of-service attacks (DDoS), which can shut down large computer servers, disrupting financial transactions and other business functions, as well as other means to exploit computer network vulnerabilities (Cilluffo, Berkowitz, and Lanz, 1998).

Invasions of computer security by hackers and other cybercriminals pose a costly threat (Manion and Goodrum, 2000). The "Melissa" virus of 1999, for example, caused damage estimated at $399 million; the financial toll from the "Love Bug" virus of 2000 was estimated as high as $10 billion (Lovelace, 2000). On February 8, 2000, a cyberhacker attacked Yahoo, Amazon, eBay, CNN, and Buy.com, closing them for several hours. The perpetrator, known as "mafia-boy," used a "distributed-denial-of-service" (DDoS) attack against these popular e-commerce Web sites (Anonymous [b] 2000: A1). In order to mount a DDoS attack, the perpetrator first breaks into a weakly-secured computer server, then installs special software on the server. When the attacker is ready, he or she sends a command via the installed software to all the "captured" machines connected to the server, instructing them to immediately send streams of requests to log onto the target Web site address. Such attacks, originating from hundreds of independent computers, eventually "flood" the targeted Web site with millions of simultaneous requests. This increase in fake service requests effectively blocks legitimate users from accessing the site (Denning, 1999: 235–239).

Malicious viruses and DDoS attacks are not the only forms of cyberterrorism, however. Cyberterrorists have also used their computer skills to extort huge sums of money from large financial institutions. They usually break into a bank's computer system and leave a message that will be found by the bank's computer security specialists, threatening to destroy the bank's computer files if specific sums of money are not sent to the terrorists.

According to a source in Great Britain, terrorists have extorted up to 400 million British pounds from 1993 to 1995 by making intimidating threats to various financial institutions.

> Over the three years, there were 40 reported threats made to banks in the U.S. and Britain. . . . In January of 1993 . . . a brokerage house paid out 10 million pounds after receiving a threat and one of their machines crashed . . . a blue chip bank paid to blackmailers 12.5 million pounds after receiving threats . . . another brokerage house paid out 10 million pounds. (Anonymous [c], 1997)

Another use of computer technologies that terrorists can exploit is called "information warfare," which "consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, object, or victory over an adversary" (Schwartau, 1994: 12). Both state and non-state actors have utilized this potentially threatening form of warfare.

In the Gulf War, for example, the United States implanted viruses and made other computer intrusions into Iraqi air defenses. And in the war against Serbia, the U.S. military "strove to distort information Serb gunners saw on their screens, helping keep U.S. planes safe during their bombing runs" (Arquilla, 2000: 16).

Terrorists now have at their disposal powerful "weapons of mass disruption" such as computer viruses, DDoS attacks, and information warfare. Will terrorists escalate their attacks in the future by using weapons of mass destruction? Of the three types of weapons of mass destruction, nuclear weapons pose the greatest potential danger (as mentioned in Chapter 2), followed by biological weapons and chemical weapons. Biological weapons are more deadly than chemical weapons.

Nuclear weapons require a complex body of knowledge, along with sophisticated technologies, raw materials, and, of course, capital, making their acquisition beyond the capabilities of all but governments. Biological and chemical weapons, however, are relatively cheaper and easier to build, provided the raw materials can be obtained, and their potential to inflict a high number of casualties should not be underestimated. For example, former U.S. Secretary of Defense William Cohen has said that a supply of anthrax the size of a 5-pound bag of sugar, properly weaponzied, would kill half the population of Washington, D.C. (Lluma, 1999: 14). Historical experience, limited as it is, is enough to arouse substantial anxiety about biochemical terrorism. For example, the use of mustard gas during WWI was sufficiently alarming to pave the way for the 1925 Geneva Protocol, prohibiting gas and bacteriological warfare.

In the late 1980s and early 1990s there were reports of Iraqi leader Saddam Hussein using chemical weapons against Kurds, Iraqi citizens whose long quest for independence made them enemies of the Iraqi government. In March of 1988, during the Iran-Iraq war, Iraqi forces used mustard gas and nerve toxins on Kurdish towns, allegedly killing approximately 5,000 people (Anonymous [d], 1988: 2). Shiite dissidents have also been the targets of chemical attacks by Saddam Hussein (Anonymous [e], 1993: A22). Assuming these reports are valid, especially the repeated attacks on the Kurds, these attacks are not only in violation of the 1925 Geneva Protocol, but they are also in violation of the 1951 Genocide Treaty, prohibiting the deliberate destruction of a particular group of people.

A Japanese terrorist group, Aum Shinrikyo, had sought to use chemical and biological weapons between 1990 and 1993. This Japanese cult subscribed to an apocalyptic vision. Its founder, Shoko Asahara, prophesied that the United States would attack Japan with nuclear weapons and destroy 90 percent of its population. To avert this catastrophe, he asserted that 30,000 followers must be recruited to ward off the eventual Armageddon. Between 1990 and 1993 this sect attempted, on at least nine different occasions, to spread biological agents in the vicinity of Tokyo and nearby U.S. military bases. Its deadliest and most well-known attack was in March of 1995, when it released sarin in a Tokyo subway, killing 12 people and injuring more than 1,000 (Kaplan, 2000: 207–226).

A comprehensive study by the U.S. General Accounting Office (GAO) has identified an array of biological and chemical agents that might be used by terrorists. The GAO report examines the technical ease or difficulty on the part of terrorists to acquire, process, improvise, and deploy chemical and biological agents to cause at least 1,000 casualties without the assistance of a government-sponsored program (see Figures 5–3 and 5–4).

Shanksville, Pennsylvania:

- United Airline, flight 93: 44 killed.

In addition to the 265 people who lost their lives on the hijacked airplanes, approximately 3,014 lives were destroyed in the twin towers of the World Trade Center and in the Pentagon. This catastrophe, as of the middle of September 2001, had also taken an enormous financial toll of $60 billion in direct costs to the U.S. economy, and approximately $600 billion in stock-market losses (Scherer and Paulson, 2001: 1). The events of September 11 have forced us to confront the monstrous reality of terrorism, and have led to a heightened state of awareness of the potentially destructive power of diverse terrorist weapons: information, nuclear, chemical, and biological.

For many years into the 21st century, terrorists will probably seek to convert technologies, whether high-tech or low-tech, into weapons of mass destruction. The fact that one of the alleged suicide bombers, Mohammed Atta, who crashed an airplane into the World Trade Center, is suspected of trying to buy a crop-dusting airplane in order to spread biological and chemical agents bears out this threat (Settle, 2001: 3). In order to achieve a maximum amount of chaos, terrorists will probably target cultural symbols of Western Civilization in the United States and elsewhere. To forestall and ward off their criminal designs we will have to surpass terrorists in ingenuity and creativity. To defeat terrorism in the United States, according to Ullman (2001: 17), we must devote the best minds to a new Manhattan Project. Useful as such a strategy might be, a technological approach alone may not suffice. We will also have to make a commitment to eradicate the economic and political roots of terrorism.

Terrorism and Counter-Terrorism

How shall we apply our four-fold causal framework to the phenomenon of terrorism? Because of the complexities of terrorism, a multiple-perspective analysis is required, namely, the application of all four of our categories of causal analysis (Bowonder and Linstone, 1987).

Since terrorism involves a deliberate human act, one would be tempted to categorize it as an exclusively human factors problem. This, however, would not do justice to the complexities of the threat. In addition to involving a deliberate action of one or more human beings, terrorism also utilizes technical design factors since it exploits the vulnerabilities of technological systems. Penetrating the security system of a computer network, for example, requires that the terrorist understands the technical details of its operating system.

In the case of biochemical weapons, technical design factors are very much involved, namely, the relative ease of manufacturing such weapons compared to nuclear weapons.

Organizational systems factors are also involved in terrorist attacks; they require the coordination of tasks on the part of the perpetrators in planning, production, and implementation of their criminal acts. For example, the events of September 11 required several years of planning and coordination among the members of the terrorist network.

Finally, socio-cultural factors are also involved in information system terrorism as well as in biochemical terrorism. Hackers may define breaching a computer security system as a technical, game-like challenge and as an opportunity to express their disdain for the authority system of corporate organizations. Their underlying motivation may be rooted in a profound alienation from the economic and legal values of a society. In the case of conventional international terrorism and biochemical terrorism, the root causes may be located in the great disparities in economic resources of developed and developing countries and in the political oppression of totalitarian regimes. Economic privation and political oppression generate widespread perceptions of injustice and resentment. Such perceptions provide the fertile grounds for hatred that eventuates in expressions of terrorism.

Our four-fold causal framework is also applicable to assessing a counter-terrorism program. Counter-terrorism involves a complex, uncertain, and costly process. It is complex because it requires attention to many dimensions of threats—chemical, biological, radiological, or nuclear; it is uncertain because it is inherently difficult to know the duration of the effort required and when, if ever, it is possible to declare victory, so to speak; and it is costly because it is an open-ended struggle necessitating the recruitment of a large number of individuals and organizations. The September 11 terrorist attacks have alerted the U.S. government and the citizenry to multiple threats. These can be categorized according to the following four counter-measures:

Technical Factor Counter-Measures

Many technical design factors have been considered as counter-terrorism measures, such as installing steel-reinforced cockpit doors on airliners. Garwin, a distinguished physicist, has advanced a number of technological proposals:

> - Ensure that the radar transponder, once switched to emergency mode by an airline pilot, cannot be switched back.
> - To counter biological warfare, individuals, firms, governments, and other organizations should consider installing a unit to provide positive pressure High Efficiency Particulate Air filter (HEPA-filtered) makeup air to their buildings.*
> - To facilitate the movement of cargo, more use should be made of the sealing of containers, ships, aircraft, or trucks at the departure point so that inspection would occur there with adequate time and space, rather than on the fly at bridges or other choke points. Electronic manifests could be sent ahead and would also accompany the vehicle. (Garwin, 2001:18)

Another technical factor counter-measure is the implementation of biometric technologies in airports, railroad stations, and anywhere else terrorists may try ro carry out their criminal plans. Biometric technologies use a person's physical characteristics to identify suspected criminals or terrorists. Digitized fingerprints, voiceprints, iris and retinal images, hand geometry, and handwritten signatures are examples of physical characteristics that can identify an individual suspected of malicious intent (Pillar and Kaplan, 2001: 3).

Although there is no high-tech silver bullet to solve the problem of terrorism, if technologies such as those noted above were used, terrorists would find it more difficult to carry out their operations.

Human Factor Counter-Measures

The U.S. government has urged the citizenry to be vigilant about possible terrorist threats. Airline pilots have urged passengers to resist attempts by terrorists to hijack airliners, and air passengers have also vowed to resist any hijackers (Verhôvek, 2001:1). In the wake of the September 11 attacks, members of Congress have sponsored a bill that would increase human responses to suspected terrorists. The bill includes having federal air marshals assigned to guard passengers and aircraft, the implementation of anti-hijack training for flight crews, and the arming of properly-trained pilots to protect the cockpit controls from threatening assailants (Simon, 2001). Another idea for helping ordinary citizens to get personally involved in combating terrorism is to initiate civilian defense programs to help guard critical infrastructures such as water and electric supply systems, buses, subways and rail transport, television and radio stations, and other possible targets of terrorist attacks. Such programs were active during WWII, when many concerned citizens volunteered. Such volunteerism creates a sense of common purpose and a sense of community, which may compel citizens to educate themselves about the multiple guises of terrorism (Anonymous [f], 2001: A38).

Organizational Systems Factor Counter-Measures

The events surrounding the September 11 attacks have pointed out weaknesses in U.S. intelligence-gathering capabilities, both at the national and international levels. In response to such weaknesses, an Office of Homeland Security has been

* "It takes a very small capital expenditure and a very small expenditure in power to provide a positive pressure so that normal winds will not infiltrate a building, and the anthrax spores or other microbes will be kept out. To do this the air intake to a normal building . . . should be provided with a small blower that delivers air through a High Efficiency Particulate Air filter at a rate that exceeds the leakage of air in or out of the building. Such 'makeup' air will then produce excess pressure in the building so that air flows out through any cracks or apertures, blocking any inflow of unfiltered air" (Garwin, 2001: 18).

established in the United States to coordinate the efforts of about four dozen government agencies to secure the nation's borders, protect nuclear power plants, share intelligence, secure public facilities, and fight bioterrorism. One major criticism leveled against agencies such as the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the National Security Agency (NSA)—the principal agencies whose job it is to look after national security—is their over-reliance on high-tech surveillance items such as satellites and spy planes, which can monitor actions on the ground, and electronic eavesdropping systems that can intercept and decipher fax, telephone, and e-mail communications throughout the world. Such forms of signal intelligence, or "signet," have proven to be of limited value in light of September 11. One task for the director of the Office of Homeland Security is to conduct a thorough review of "signet" technologies. Another is to focus more attention on "humint" or human intelligence capabilities, which translates into the use of operatives on the ground who can infiltrate terrorist networks and relay information back to officials that only an "insider" can know (Pincus, 2001: A11).

Socio-Cultural Factor Counter-Measures

Congress is updating a 1996 law pertaining to biological agents and toxins that require export licenses to ensure that they do not fall into terrorist hands. There is also a proposal to have optional national ID cards, which would make it "more difficult for potential terrorists to hide in open view, as many of the September 11 hijackers apparently managed to do" (Dershowitz, 2001:A23). Such an ID card would provide a tradeoff: a reduction in privacy for an increase in security.

Paradoxically, many technologies that can be used to combat terrorism can also threaten our individual privacy as well as our civil liberties. Civil libertarians claim that it is against our constitutional rights to have our biometric information analyzed and put in a database without our consent. Another example is the use of DNA to combat crime. The same DNA databases that can be used to identify and convict suspected criminals could also be used to identify genes associated with certain physical and mental health conditions that sufferers might wish to keep private. Do we want to live in a society where law enforcement personnel have the ability to monitor citizens' comings and goings by means of national ID cards, scan large crowds with face-recognition technologies in an attempt to identify known criminals, and have access to DNA databases that contain information individuals wish to keep out of the hands of employers and insurance companies? These technologies can certainly be used to combat terrorism, but they also conjure up dystopian fears of "Big Brother" and a loss of privacy and freedom. What is needed is a concentrated effort to educate the public about such technologies and a process of democratic deliberation over their possible uses. If such technologies are put to use with little or no public debate, it will create mistrust in the citizenry. In order to take advantage of surveillance technologies such as national ID cards, biometrics, or DNA databases, public debates are essential and a democratic consensus needs to be achieved—this is the only way such technologies can be made consistent with the cultural values of individual freedom and democracy that are central to our way of life.

Conclusion

To explain terrorism and to assess counter-terrorism programs in the nuclear-information age, we have drawn on the combined conceptual power of our four root causes of technological disasters. In discussing these causes of technological disaster, we assumed that they were applicable independent of time and place. In Chapter 6, we attempt to provide a context for technological disasters by placing them in an historical framework—the three industrial revolutions. What our investigation reveals is that the four root causes discussed in this chapter throw light on the course of technological development.

References

Anderson, Robert M., Schendel, Dan E., and Trachtman, Leone E. (1980). *Divided loyalties: Whistleblowing at BART.* Purdue, IN: Purdue Research Foundation.

Anonymous (a). (2001). "The Kansas City Hyatt Regency walkways collapse," Department of Philosophy and Department of Mechanical Engineering, Texas A&M University. Accessed from the World Wide Web at: http://lowery.tamu.edu/ethics/ethics/hyatt/hyatt1.htm

Anonymous (b). (2000). "Fifteen year old accused in CNN case," *The Houston Chronicle,* Thursday, April 20: A1.

Anonymous (c). (1997). Accessed from the World Wide Web at: www-cs.etsu.tn.edu/gotterbarn/stdntppr/stats.htm. "Statistics on Cyber-terrorism."

Anonymous (d). (1988). "Iraq chemical attacks kill Kurds," *The Financial Times* (London), April 2: 2.

Anonymous (e). (1993). "Hundreds of Shiites reported killed by Iraqi chemicals," *The Toronto Star,* October 23: A22.

Anonymous (f). (2001). "Turn again to civil defense," *The Washington Post,* September 28: A38.

Arquilla, John. (2000). "Preparing for cyberterrorism—badly," *The New Republic,* May 1: 16.

Baron, S. (Ed.). (1990). *Quantitative modeling of human performance in complex, dynamic systems.* Washington, DC: National Academy Press.

Baskin, O., and Aronoff, C. (1988). *Interpersonal communication in organizations.* Santa Monica, CA: Goodyear Publishing Co.

Betts, Mitch. (1994). "Pentium flaw joins long list of computer math mistakes," *Computerworld,* December 19; 28 (51): 4.

Bignell, V., and Fortune, J. (1984). "Human factors paradigm." Chapter 12 in *Understanding systems failures.* Manchester, UK: Manchester University Press: 190–205.

Bondurant, S., Ernster, V., and Herdman, R. (Eds.). (2000). *Safety of silicon breast implants.* Committee on the Safety of Silicon Breast Implants. Washington, DC: Institute of Medicine.

Bowonder, B., and Linstone, H.A. (1987). "Notes on the Bhopal accident: Risk analysis and multiple perspectives," *Technology Forecasting and Social Change* 32: 183–202.

Chase, Alston. (2000). "Harvard and the making of the Unabomber," *The Atlanta Monthly* 285 (6): June: 41–65.

Cilluffo, Frank, Berkowitz, Bruce, and Lanz, Stephanie (Eds.). (1998). *Cybercrime, cyberterrorism and cyberwarfare.* Washington, DC: The Center for Strategic and International Studies.

Clothier, Norman. (1987). *Black valor: The South African native labor contingent, 1916–1918, and the sinking of the Mendi.* Pieternaritzburg, South Africa: University of Natal Press.

Corman, S., Mayer, Michael E., Bantz, Charles R., and Banks, Stephen P. (Eds.). (1990). *Foundations of organizational communication: A reader.* New York: Longman Press.

Denning, Dorothy. (1999). *Information warfare and security.* Boston, MA: Addison-Wesley.

Dershowitz, Alan M. (2001). "Why Fear National ID Cards," *The New York Times,* October 13: A23.

Dombrowski, P. (1992). "Challenger and the social contingency of meaning," *Technical Communication Quarterly* 1 (3).

Dumas, Lloyd. (1999). *Lethal arrogance: Human fallibility and dangerous technologies.* New York: St. Martin's Press.

Farley, C.J. (1995). "The man who wasn't there (world trade center bombing arrest)," *Time,* February 20: 24.

Fisher, A. (1986). *Small group decision-making: Communication and the group process.* New York: McGraw-Hill.

Garwin, Richard L. (2001). "The many threats of terror," *The New York Review of Books* Vol. XLVIII (November 1, 2001): 16–19.

Glegg, Gordon L. (1971). *The design of design.* Cambridge, England: Cambridge University Press.

Gouran, D., Hirokawa, R., Martz, A. (1986). "A critical analysis of factors related to decisional processes involved in the Challenger disaster," *Central States Speech Journal* 37 (3): 119–135.

Grove, Andrew S. (1996). *Only the paranoid survive: How to exploit the crisis points that challenge every company and career.* New York: Doubleday Books.

Grove, Andrew S. (1998). "My biggest mistake," *Inc.,* May 20 (6): 117.

Hartley, Robert. (1993). "Dow Corning and silicone breast implants: Another Dalkon Shield?" In Robert Hartley, *Business ethics: Violations of the public trust.* New York: John Wiley & Sons: 235–251.

Herndl, C., et al. (1994). "Understanding failures in organizational discourse: The accident at Three Mile Island and the shuttle Challenger disaster." In C. Bazerman (Ed.), *Textual dynamics of the professions.* Milwaukee: University of Wisconsin Press.

Hirokawa, R., Gouran, D., Martz, A. (1988). "Understanding the sources of faulty group decision-making: A lesson from the Challenger disaster," *Small Group Behavior* 19 (4): 411–433.

International Atomic Energy Agency. (1986). *Yearbook 1986.* Vienna: International Atomic Energy Agency: 76.

International Atomic Energy Agency. (1987). *Yearbook 1987.* Vienna: International Atomic Energy Agency: 43.

Jackson, Carlton. (1982). *The dreadful month.* Bowling Green, OH: Bowling Green State University Press.

Jacky, Jonathan. (1990). "Risks in medical electronics," *Communications of the ACM* 33 (12): 138.

Janis, I. (1972). *Victims of groupthink.* Boston, MA: Houghton Mifflin.

Joyce, Ed. (1987). "Software bugs: A matter of life and liability," *Datamation* 33: 88–93.

Kaczynski, T. (1995). "Excerpts from the Unabomber's manifesto," *The Washington Post,* August 2: A16.

Kaplan, D. (2000). "Aum Shinrikyo." In Jonathan Tucker (Ed.), *Toxic terror: Assessing terrorist use of chemical and biological weapons.* Cambridge, MA: MIT Press: 207–226.

Kerstetter, Jim. (2000). "How many 'love bugs' will it take?" *Business Week,* May 22: 50–56.

Landau, Martin, and Stout, Russell. (1979). "To manage is not to control: Or the folly of type II errors," *Public Administration Review,* March/April; 148–156.

Lawrence, Anne. (1993). "Dow Corning and the silicone breast implant controversy." In John Boatright (Ed.), *Cases in ethics and the conduct of business.* Englewood Cliffs, NJ: Prentice Hall: 237–263.

Leveson, Nancy, and Turner, Clark. (1993). "An investigation of the Therac-25 accidents," *Computer* 26 (7): 18–41.

Lluma, Diego. (1999). "Low probability, high consequence: Biological terrorism," *Bulletin of the Atomic Scientists* 55 (6): 14.

Lopez, Steve. (2001). "Tighter airport security is just a flight of fancy," *Los Angeles Times,* October 5: A1.

Lovelace, Herbert. (2000). "A clear and present danger," *Informationweek,* May 22: 166–173.

Manion, M., and Goodrum, A. (2000). "Terrorism of civil disobedience?: Towards a hacktivist ethic," *Computers and Society* 20, June: 14–19.

Martin, M., and Schinzinger R. (1996). *Engineering ethics* (3rd ed.). New York: McGraw-Hill.

Mendlovitz, Saul. (2001). "Crime(s) of terrorism: Developing law and legal institutions," *Newsletter of the Lawyers' Committee on Nuclear Policy* (Fall) 13 (2): 3.

Meshkati, N. (1991). "Human factors in large-scale technological systems' accidents: Three-mile island, Bhopal, and Chernobyl," *Industrial Crisis Quarterly* 5: 131–154.

Meshkati, N. (1992). "Ergonomics of large-scale technological systems," *Impact of Science on Society* 42 (165): 87–97.

Miller, C. (1993). "Framing arguments in a technical controversy: Assumptions about science and technology in the decision to launch the space shuttle Challenger," *Journal of Technical Writing and Communication* 23 (2): 99–144.

Moore, P. (1992). "When politeness is fatal: Technical communications and the Challenger accident," *Journal of Business and Technical Communication* 6 (2): 269–292.

Nader, Ralph, and Smith, Wesley J. (1993). *Collision course: The truth about aviation safety.* New York: McGraw-Hill: 294–295.

Neumann, Peter. (1989). "Risks to the public in computers and related systems," *Software Engineering Notes* 14 (1): 6–21.

Neumann, Peter. (1995). *Computer-related risks.* New York: ACM Press; Reading, MA: Addison-Wesley.

Nixon, P., and Frost, M. (1975). "Choosing a factor of safety." In R.R. Whyte (Ed.), *Engineering progress through trouble.* London: The Institution of Mechanical Engineers: 136–141.

Norman, Colin. (1986). "Chernobyl: Errors and design flaws," *Science,* September 5; 233: 1029–1033.

O'Hara, J. (1996). "Human factors evaluation of advanced nuclear power plants." In T. O'Brien (Ed.), *Handbook of human factors testing and evaluation.* Mahwah, NJ: Lawrence Erlbaum Publishers.

Pace, R. (1988). "Technical communication, group differentiation, and the decision to launch the space shuttle Challenger," *Journal of Technical Writing and Communication* 18 (3): 207–220.

Petroski, Henry. (1985). *To engineer is human: The role of failure in successful design.* New York: St. Martin's Press.

Petroski, Henry. (1994). *Design paradigms: Case histories in error and judgment in engineering.* Cambridge, UK: Cambridge University Press.

Pillar, Charles, and Kaplan, Karen. (2001). "America attacked: Technology implications; technology tools," *Los Angeles Times,* September 12: 3.

Pillar, Paul R. (2001). *Terrorism and U.S. foreign policy.* Washington, DC: Brookings Institution Press.

Pincus, Walter. (2001). "House panel suggests revamping intelligence," *The Washington Post,* October 2: A11.

Pinsky, Robert. (1990). "Shirt," *The want bone.* New York: Farrar, Straus and Giroux.

Redmill, F. (Ed.). (1997). *Human factors in safety critical systems.* Boston, MA: Butterworth-Heinemann.

Renz, M.A., and Greg, J. (1988). "Flaws in the decision-making process: Assessment of risk in the decision to launch Flight 51-L," *Central States Speech Journal* 39 (1): 67–75.

Rochlin, G. (1991). "Iran Air Flight 655 and the USS Vincennes: Complex, large-scale military systems and the failure of control." In T. Laporte (Ed.), *Social responses to large technical systems.* Dordrecht, Netherlands: Kluwer Academic Publishers: 99–125.

Roddis, W.M. Kim. (1993). "Structural failures and engineering ethics," *Journal of Structural Engineering* 119 (5): 1539–1555.

Rowland, R. (1986). "The relationship between the public and the technical spheres of argument: A case study of the Challenger disaster," *Central States Speech Journal* 37 (3): 134–146.

Salecker, Gene. (1996). *Disaster on the Mississippi: The Sultana explosion, April 25, 1865.* Annapolis, MD: Naval Institute Press.

Scherer, Ron, and Paulson, Amanda. (2001). "Costliest Disaster in U.S. history," *The Christian Science Monitor,* September 20: 1.

Schwartau, Winn. (1994). *Infowarfare: Cyberterrorism: Protecting your personal security in the information age.* New York: Thunder's Mouth Press.

Sciolino, Elaine, and Gordon, Michael. (2000). "Ukraine consents to shut Chernobyl before years end," *The New York Times,* June 6: A1.

Serrill, Michael. (1986). "Anatomy of a catastrophe: Moscow blames 'gross' human error for the Chernobyl accident," *Time,* September 1; 128: 26–30.

Settle, Michael. (2001). "Terrorist tried to buy crop-duster aeroplane," *The Herald* (Glasgow), September 26: 3.

Shcherbak, Yuri. (1996). "Ten years of the Chernobyl era," *Scientific American* 274(4): 44–54.

Shrivastava, P., Mitroff, I., Miller, C., and Miglani, R.I. (1988). "Understanding industrial crises," *Journal of Management Studies* 25 (4): 285–303.

Simon, Richard. (2001). "Aviation bill clears U.S. Senate," *Los Angeles Times,* October 12: A8.

Starbuck, W., and Milliken, F. (1988). "Challenger: Fine-tuning the odds until something breaks," *Journal of Management Studies* 25 (4): 319–340.

Stein, Leon. (1962). *The triangle fire.* Philadelphia, PA: J.B. Lippincott.

Stolberg, Sheryl. (2001). "Study links breast implants to lung and brain cancers," *The New York Times,* April 26: 36.

Sweet, William. (1989). "Chernobyl: What really happened?" *Technology Review* 92: 43–52.

Turner, B. (1984). *Man-made disasters.* London: Wykam Press.

Ullman, Harlan. (2001). "Intellect over intelligence," *The Financial Times,* October 19: 17.

Vandivier, K. (1972). "Why should my conscience bother me?" In M. David Ermann and Richard J. Lundman (Eds.), *Corporate and governmental deviance: Problems of organizational behavior in contemporary society.* New York: Oxford University Press: 205–226.

Vaughn, Diane. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA.* Chicago, IL: University of Chicago Press.

Verhovek, Sam Howe. (2001) "Air passengers vow to resist any hijackers," *The New York Times,* October 11: 1.

Whetzel, D. (Ed.). (1997). *Applied measurement methods in industrial psychology.* Palo Alto, CA: Davis-Black Publishers.

Whyte, R.R. (1975). *Engineering progress through trouble: Case histories drawn from the proceedings of the Institution of Mechanical Engineers.* London: Institution of Mechanical Engineers.

Wiener, E. (Ed.). (1988). *Human factors in aviation.* San Diego, CA: Academic Press.

Williams, Cindy. (1997). "Intel's Pentium chip crisis: An ethical analysis," *IEEE Transactions on Professional Communication* (March), 40 (1): 13–20.

Winsor, D. (1990). "The construction of knowledge in organizations: Asking the right questions about the Challenger," *Journal of Business and Technical Communication* 4 (2).

Witkin, Gordon, and Roebuck, Karen. (1998). "Torments that will not end: Why Terry Nichols escaped execution," *U.S. News & World Report* 124 (2), January 19: 33.

Yager, Wilson. (1976). "The Sultana disaster," *Tennessee Historical Quarterly* 35 (3): 117–132.

Yardley, Jim. (2000). "Five years after terrorist act: A memorial to the 168 victims," *The New York Times,* April 20: 16, 20.

Case Study	Terminology
USS *Princeton* Explosion	tragedy
Titanic Sinking	tragedy, disaster
Aisgill Train Wreck	disaster
Johnstown Flood	disaster, calamity
DC-10 Crash	disaster
Tenerife Runway Collision	disaster
Santa Barbara Oil Spill	accident
Love Canal Toxic Waste Contamination	disaster
Apollo I Fire	accident, disaster
Three Mile Island	accident
Challenger Disaster	disaster
Bhopal Poison Gas Release	accident

Figure 8–1
Terminology used by authors of the 12 case studies to characterize technological disasters.

Clearly, the terms used do not always convey the magnitude of disaster with regard to the loss of life and property. This is obviously the case with the Bhopal Poison Gas Release, which should certainly be called a disaster or a calamity, given that 14,000 people were killed and tens of thousands were injured. In fact, the characterization of such devastating technological disasters as "accidents" inadvertently places them in the same category as totally unexpected or totally unintentional misfortunes. The implication of falsely categorizing such technological disasters in this manner is that it:

> . . . skews our perceptions in a certain direction: We see it not only as an unintended and unanticipated event, but also as an unavoidable event—something that could not have reasonably been prevented. It also implies that what happened was an act of fate—the result of impersonal forces—and to the extent that human actions were involved, they would not be regarded as "causing" the unexpected event. The net effect of this cultural classification . . . is to obscure the role of human actions in the production of . . . disaster[s] . . . (Poveda, 1994: 21–22)

Reference

Poveda, Tony. (1994). *Rethinking white-collar crime.* Westport, CT: Praeger.

Four Root Causes of Technological Disaster

Three Industrial Revolutions		Technical Design Factors	Human Factors	Organizational Systems Factors	Socio-Cultural Factors
	First Industrial Revolution	USS *Princeton* Explosion	*Titanic* Sinking	Aisgill Train Wreck	Johnstown Flood
	Second Industrial Revolution	DC-10 Crash	Tenerife Runway Collision	Santa Barbara Oil Spill	Love Canal Toxic Waste Contamination
	Third Industrial Revolution	Apollo I Fire	Three Mile Island	Challenger Disaster	Bhopal Poison Gas Release

Figure 8–2
The 3 × 4 matrix of case studies of technological disasters, as presented in Chapter 8.

Four Root Causes of Technological Disaster

Three Industrial Revolutions		Technical Design Factors	Human Factors	Organizational Systems Factors	Socio-Cultural Factors
	First Industrial Revolution	Dee Bridge Collapse	SS *Mendi* Collision	*Sultana* Steamboat Sinking	Monongah Mine Disaster
	Second Industrial Revolution	Hyatt Regency Walkway Collapse	USS *Vincennes* (Iranian Airbus Shootdown)	B.F. Goodrich Brake Scandal	Triangle Shirtwaist Factory Fire
	Third Industrial Revolution	Therac-25 Radiation Device Malfunction	Chernobyl Disaster	BART Whistleblowing Case	Dow Corning Breast Implants

Figure 8–3
Twelve case studies of technological disasters discussed in Chapter 5, classified by the 3 × 4 matrix.

CHAPTER 9

Lessons Learned from the Case Studies of Technological Disasters

"It is important to acknowledge mistakes and make sure you draw some lessons from them."

—Bill Gates

A startling fact emerges from the 12 exemplary case studies of technological disasters presented in Chapter 8: Many of the cases of technological disaster considered in that chapter, as well as those discussed in Chapter 5, could actually have been prevented! Indeed, an argument can be made that many of the technological disasters could have been anticipated on the basis of what experts and executives in the various industries involved already knew. According to the civil engineer Henry Petroski, "the greatest tragedy underlying design errors and the resultant failures is that many of them do indeed seem avoidable, yet one of the potentially most effective means of improving reliability in engineering appears to be most neglected" (Petroski, 1994: ix)—namely, the critical importance of studying disasters.

SPECIFIC LESSONS LEARNED

An analysis of the various case studies of technological disaster presented in Chapters 5 and 8 yields sets of specific lessons to be learned (see Figures 9–1 and 9–2). By identifying and classifying

Case Studies	Lessons Learned
1. USS *Princeton* Explosion	1. Marked deviation from design standards for naval guns led to weaknesses in the barrel, resulting in an explosion during firing.
2. *Titanic* Sinking	2. Overconfidence in technology creates a sense of omnipotence and lack of vigilance.
3. Aisgill Train Wreck	3. Human resource management failure and rigid management scheduling stemmed from preoccupation with maximizing profits.
4. Johnstown Flood	4. Shoddy construction standards reflected callous attitudes of owners of fishing club toward subordinate social classes.
5. DC-10 Crash	5. FAA's regulatory failures to control design problems of aircraft manufacturers and reluctance to issue airworthiness directives grounding defective aircraft until repairs were made.
6. Tenerife Runway Collision	6. Miscommunication among pilots and air flight controllers and inability to control stress and anxiety paved the way for the collison.
7. Santa Barbara Oil Spill	7. Corporate power of oil companies subordinated public considerations of health and safety to its own calculus of profits.
8. Love Canal Toxic Waste Contamination	8. School board and community organizations failed to appreciate health hazards of toxic chemicals, and the polluting corporation covered up its irresponsible behavior to limit liability and malfeasance.
9. Apollo I Fire	9. Faulty wiring by contractors combined with failure of NASA personnel to use proper methods of cabin pressurization.
10. Three Mile Island	10. Complexity of technology increased the fallibility of human judgment.
11. Challenget Disaster	11. Conflicting agendas of NASA and Morton Thiokol management and engineers led to faulty risk assessment and decision making.
12. Bhopal Poison Gas Release	12. Depreciation of the value of life in a Third World country justified cutting corners in the design of the plant, including laxness of safety standards.

Figure 9–1
Specific lessons learned from the case studies of technological disasters presented in chapter 8.

Case Studies	Lessons Learned
1. Dee Bridge Collapse	1. Extension of design beyond known limits and past successes in design breed failure.
2. Hyatt Regency Walkway Collapse	2. Engineers fail to conform to acceptable practice in communicating "design intent" to contractors; imprudent deviation from original design of connection structures linking the two walkways.
3. Therac-25 Computer Malfunction	3. Design defects in the computer system; insufficient testing failed to identify avoidable bugs in the computer program.
4. SS *Mendi* Collision	4. Reckless behavior of the captain on the high seas caused two ships to collide; noncompliance with regulations to come to the aid of distressed ships at sea caused the death of 800 military personnel.
5. USS *Vincennes* Failure	5. Human-computer interaction failure; operational difficulties in the interpretation of the hyper-complex computer system AEGIS, under stress of battle, led to operator anxiety, task fixation, and unconscious distortion of facts.
6. Chernobyl Nuclear Catastrophe	6. A poorly designed graphite-moderated nuclear reactor, accompanied by numerous violations of operating procedures, careless disablement of safety systems, and reckless operator judgments led to the disaster.
7. *Sultana* Sinking	7. Laxity in the enforcement of safety standards provided a climate of carelessness, negligence, and bad judgments: 1,800 men are loaded onto a steamboat with the capacity of 376. Excessive weight put stress on the boilers, which exploded, sinking the boat. Ignorance of boiler safety standards was also responsible for the failure.
8. B.F. Goodrich Brake Scandal	8. Elite engineers were involved in a conspiracy to falsify data and develop a scheme of deception to protect firm's contract with the U.S. Air Force.

Figure 9–2
Specific lessons learned from the case studies of technological disasters presented in chapter 5.

Case Studies	Lessons Learned
9. BART System Malfunctions	9. Automated control system was found to have major design flaws; testing and operator training was inadequate; major software bugs plagued the computerized transit system.
10. Monongah Mine Explosion	10. Ignorance of safety issues and lack of enforceable safety regulations were primarily responsible for the mine disaster.
11. Triangle Shirtwaist Factory Fire	11. Gross violations of building safety codes and callous disregard for immigrant workers were significant causes of the fire.
12. Dow Corning Breast Implants	12. Distorted cultural values concerning the female body image, inadequate regulatory control over medical devices, and the company's withholding of data of known dangers of breast implants all contributed to the implant failure.

Figure 9–2 ***(continued)***

the causes and lessons of technological disasters, we create a fund of ideas for better technology assessment and technology management.

If an analysis of the case studies of technological disasters helps identify known hazards associated with various technologies, the obvious questions arise: Why were the known risks not adequately taken into account? Why were steps not taken to prevent them? These case studies reveal that time and again, the same or similar mistakes have led to technological disasters. This insight has led us to develop our four root causes of technological disaster. It is our thesis that the analysis of case studies is the key to understanding the nature of technological disasters. Studies of failures provide opportunities for design engineers and organizational analysts concerned with technology management to heed the lessons learned and hence to avoid making similar errors in the future. If design engineers, organizational planners, and policymakers—those who decide how organizational structures, machines, and other technological systems are designed and built—would study technological disasters with the same systematic approach given to the studies of technological successes, they could greatly improve the reliability of the technological systems they design, implement, and manage.

General Lessons Learned

One obvious lesson is that we *can* learn from technological disasters, provided that design engineers and technology management specialists share important information about past failures. Unfortunately, this seemingly obvious point is often neglected. Also neglected are human factors, such as those identified by Glegg, a specialist in engineering design:

> . . . we may forget that a 'designer' or 'engineer' is first and foremost a human being. A human being who designs or engineers has, in additon, a wide range of complicated and interacting emotions. It is easy to become emotionally involved in a new invention and so resent criticism of it even when that criticism, if heeded, would turn a failure into a success. (Glegg, 1971: 92–93)

Organizations that manage high technology all too often focus on narrow and disparate goals, overlooking the perspectives of the full cast of stakeholders or constituencies involved. Commercial goals of economy and efficiency often trump values of safety and the public good. As Roger McCarthy, principal engineer for Failure Analysis Associates—one of the premier engineering firms that investigates technological failures—points out, "The systems that involve huge energy reservoirs and therefore the highest potential for catastrophic accidents are also the ones where huge amounts of capital are tied up" (Roush, 1993: 52). In other words, since billions of dollars are tied up in the industrial production of oil, chemicals, transportation, electricity, nuclear power, etc., it is often difficult—sometimes practically impossible—to hold these industries fully accountable for their neglect of safety because of the power and influence they wield in our industrialized civilization. This fact leads to "organizational inertia" concerning the proper management of technology and the "institutional neglect of low probability, high consequence events" (Roush, 1993: 54).

A few examples will advance the argument that lack of shared knowledge concerning failures impedes the ability of stakeholders to learn from past mistakes and, as a result, leaves them unprepared to fully understand how and why technological disasters happen. The reason why so many people perished in the *Titanic* tragedy was the inadequate number of lifeboats. In fact, the *Titanic* lacked a sufficient number of lifeboats decades *after* most of the passengers and crew of the steamship *Arctic* perished because of the same problem (Martin and Schinzinger, 1996: 80). On May 15, 1980, a ship rammed the Tampa Bay Skyline Bridge. The bridge subsequently collapsed, eventually killing 13 people. This disaster, "was the largest and most tragic of a growing number of incidents of ships colliding with bridges over navigable waterways" (Martin and Schinzinger, 1996: 83). Other notorious ship-bridge collisions are the Maracaibo Bridge (Venezuela, 1964) and the Tasman Bridge (Australia, 1975). The Tampa Bay Skyline Bridge collapsed when hit by a ship because the bridge was not designed with horizontal impact forces in mind—the same engineering cause at the center of all of the bridge failures mentioned (Martin and Schinzinger, 1996: 82). According to Martin and Schinzinger, horizontal impacts were not considered simply because the relevant codes did not require it.

It is well known, of course, that valves are notoriously unreliable components of hydraulic systems. Yet, a pressure relief valve, and "lack of definitive information regarding its open or shut state," contributed to the nuclear reactor accident at Three Mile Island on March 28, 1979 (Martin and Schinzinger, 1996: 83). Similar malfunctions had occurred with identical valves on another nuclear reactor just six months earlier at the Toledo, Ohio, nuclear power plant. The required reports of malfunction were filed with Babcock and Wilcox, the manufacturer of both the Toledo reactor and the reactor at Three Mile Island. However, the manufacturers failed to share the information with the managers at Three Mile Island (Martin and Schinzinger, 1996: 84).

Problems of communication and/or mismanagement need to be overcome and replaced with open discussion and debate about design and other engineering failures in order to prevent repeating similar mistakes in the future. The few examples just discussed are hardly an exhaustive account of past disasters that tragically did not prompt technologists, managers, and policy makers to heed important lessons. They are illustrative of a telling point that "ignorance is the father of disaster, a father whose progeny multiply hideously when powerful, complex technologies are involved" (Mark, 1987: 49).

In fact, John Kemeny, Chairman of the Presidential Commission on TMI, points to individual and organizational failures to learn from past disasters as crucial factors that led to the TMI accident.

> Of the three 'people problems' [discussed earlier], I saved the Nuclear Regulatory Commission for last. I have to report to you that the agency . . . was a total disaster. It was clearly not part of the solution but a serious part of the problem . . . they had no systematic way—I mean that absolutely literally and I am repeating sworn testimony by senior NRC officials—*they had no systematic way of learning from experience.* It was an agency convinced that the equipment was so foolproof that nothing bad could possibly happen . . . (Kemeny, 1980: 69)

Our analyses of case studies in Part IV, as well as the discussions of numerous case studies throughout the book, provide an opportunity for improving the safety of technological innovations. This is achieved by alerting design engineers and organizational and policy planners to common pitfalls in the design, management, and diffusion of technological systems—something that must begin with the study of failures. According to Petroski, "the concept of failure is central to the design process, and it is by way of thinking in terms of obviating failure that successful designs are achieved" (Petroski, 1985:1). Petroski's point is that an engineering or technological disaster often can serve as a powerful stimulus for the development and creation of new engineering knowledge.

The examination of a failed technology frequently brings to the fore previously unknown, underestimated, or neglected variables concerning the materials and components. These generally remain concealed or even suppressed until a system failure forces a reexamination of existing scientific and technical knowledge. This can induce a reevaluation of the technology, followed by adjustments and corrections of errors. While technological failures and disasters have a variety of negative consequences, in some instances the lessons they generate, if heeded, may improve the standards and safety of technological systems.

The *Titanic* sinking, for example, led to unprecedented international regulations and the development of international organizations concerned with safety on the high seas. Starting in 1913, two years after the *Titanic*'s sinking, a series of annual conferences were convened on the Safety of Life at Sea (SOLAS). Also in 1913, the International Ice Patrol (IPP) was formed. The IPP is still in operation, now using sophisticated equipment such as aerial surveillance, satellite images, and radio-equipped oceanographic drifter buoys to detect icebergs (Tenner, 1997: 330).

Consider another example: After the Apollo I fire, NASA made hundreds of modifications, including the installation of higher quality wiring and flameproof coatings over all wire connections, as well as the removal of virtually all flammable materials from inside the module. A new fire-resistant material known as Beta cloth was developed for astronauts' spacesuits. Finally, adjustments were made that required the cabin to be filled with a combination of nitrogen and oxygen, instead of pure oxygen, as was the case with the Apollo I (Van Duyne, 1994).

Such case studies are rife with lessons to be learned from technological disasters. A new technology, once developed and used, is first evaluated for success. The accompanying perceptions are that a technology, once developed and accepted as safe, becomes a standard and permanent addition to our technological civilization. In fact, this was the perception of NASA engineers and scientists when they evaluated the success of the unmanned Gemini flights and decided to send manned missions into space with the introduction of the Apollo program. When a technological innovation unexpectedly proves to be defective, it shatters our convictions about the dependability of our handiwork. It forces us to reevaluate the components of the technological achievement. In the course of reevaluating the technological components, scientists and engineers are compelled to redevelop or reengineer the innovation. This suggests a cycle, as shown in Figure 9–3.

The cycle of technological development—success→failure→reevaluation→reengineering—is illustrated in many of our cases involving technical design defects. A successful engineering development is often generalized and becomes a standard for engineering practice—until an unexpected failure occurs. Engineers and applied scientists need to become sensitive to such cycles because, to paraphrase the philosopher George Santayana: those who ignore the lessons of technological disasters are bound to repeat them.

It is crucial that such learning from technological disasters becomes routine in industry operations and engineering school education. As Roush points out:

> A society facing a technological disaster is presented with a choice: whether to repair the technology in question and get on

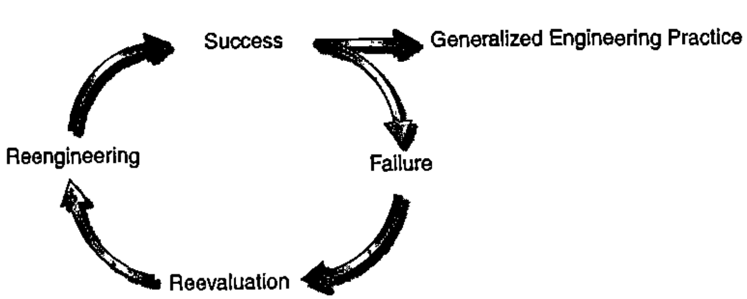


Figure 9–3
Engineering design cycle of success and failure.

> with life as quickly as possible, or whether to use the facts brought to light to map out the ways in which the society depends on that technology, the extent to which these needs are legitimate, and how they might be met more safely or fairly. (1993: 50)

Hence, it behooves technologists and policy makers to take heed of the engineering design cycle presented in Figure 9–3. Only if we can identify patterns that lead to technological disaster can we learn to prevent them. With the aid of such knowledge we can come to a better collective understanding about the social role of technology and its positive, as well as negative impacts. Along with Roush (1993), we would like to point out that we have at least two choices. We can submit the lessons learned from technological disasters to scientific scrutiny, cataloguing and classifying, developing theories as to their origins, causes, and mitigation. We could also participate in widespread public debate over their significance, involving legislators, corporate executives, public interest groups, and concerned citizens. However, we can also simply close our eyes to the consequences and lessons of technological disasters. We can decide to write them off as unavoidable "externalities" associated with technological "progress." We can ignore the lessons learned, or we can realize how crucial such lessons can be for the proper management of technology.

Now, as we argued previously, the functioning of our sociotechnical systems involves a complex web of factors—technical, human, organizational, and socio-cultural—each involving perhaps hundreds of separate items and all subject to failure. In order to identify the relevant actors involved, failure analysis must extend beyond mere technical causes. Taking full advantage of the lessons learned from technological failures and disasters would require extending the analysis to the human factors, organizational factors, and socio-cultural factors.

As technology becomes more complex and its scope becomes wider, human factors become increasingly more crucial in terms of a technology's success or failure. Large-scale technologies are so complex that simple inattention, human error, poor training, or miscommunication may become causes of potentially destructive failure. This was evident in the case of Three Mile Island, where the complexity of technology increased greatly the fallibility of human judgment, especially when coupled with human inattentiveness, inadequate training, confusion, and miscommunication. The Presidential Commission acknowledged that human causes of the Three Mile Island accident were evident at all levels: operational, managerial, and regulatory. As the report states:

> We are convinced that if the only problems were equipment problems, this Presidential Commission would never have been created . . . but wherever we looked, we found problems with the human beings who operate the plants, with the management that runs the key operation, and with the agency that is charged with assuring the safety of nuclear power plants. . . . To prevent nuclear accidents as serious as Three Mile Island, fundamental changes will be necessary in the organization, procedures, and practices, and above all, in the attitudes of the Nuclear Regulatory Commission; and to the extent that the institutions we investigated are typical, of the nuclear industry. (Peterson, 1982: 36)

Additional case studies provide ample lessons to be learned about the role of human factors in generating technological disasters. The Tenerife runway collision illustrates the disastrous consequences of individuals' inabilities to handle the stress and anxiety that often accompany the operation of complex technologies and teach us about the vulnerabilities of human attempts to manage such technologies. The same lessons can be learned from the shooting down of the Iranian airliner by the USS *Vincennes,* as well as the negligent operations and management of the Chernobyl nuclear power plant.

Technological disasters also teach us that we must be alert to the unanticipated side effects of technological innovations (Tenner, 1997). Some of the unintended consequences of technology have the potential for mass destruction of natural habitats and other types of environmental and ecological destruction. Chernobyl, Exxon *Valdez,* Bhopal, Love Canal, and the Santa Barbara

Oil Spill are all cases in point. Less dramatic, but certainly more potentially destructive, are the phenomena of global warming and the depletion of the ozone layer (Anonymous, 1998; Kerkin, 2000; Houlder, 2000).

Such unintended consequences often point to lessons that can be learned if the organizations involved in the development of technology, along with the influence of the profit motive on their operations, are made transparent (Tenner, 1997: 310). In the Love Canal and Bhopal cases, for example, we discover that instead of being designed and operated to be safety-promoting, the systems in question end up being error-inducing. Tenner concludes that:

> The real question is not whether new disasters will occur. Of course they will. It is whether we gain or lose ground as a result. It is whether our apparent success is part of a long-term and irreversible improvement of the human condition or a deceptive respite in a grim and open-ended Malthusian pressure of human numbers and demands against natural limits. (Tenner, 1997: 348)

As we have pointed out in Chapter 4, human beings do indeed have the capacities to successfully manage technology in a variety of ways—as in the case of High Reliability Organizations. One way is to focus on what lessons can be learned from the mismanagement of technological systems. An adequate understanding of how the lessons of failed technologies can lead to more reliable design and management strategies is possible only if the analysis is extended, as Jasanoff points out, "to the organizational, social, political and moral dimensions" of technological disasters (1991: 2). According to Jasanoff:

> There is a new emphasis on the organizational context in which the failed technology was embedded and, with this, a recognition that corrective policies have to address not only the design of artifacts but also (indeed perhaps even more so) the human practices and presuppositions that determine their management and use. Seen from this perspective, a serious technological mishap ceases to be merely accidental, for it opens windows onto previously unsuspected weaknesses in the social matrix surrounding the technology. (1991: 2)

In addition to the potential for organizational learning, technological disasters also teach us about the functioning of technology in society, the support systems surrounding it and the socio-cultural matrix of values that sustain it. The destruction following the methyl isocyanate leak at Bhopal provided important lessons about the strengths and weaknesses of communication systems, social welfare systems, and emergency preparedness operations, including search and rescue facilities (Wexler, 1990; Sethi, 1992). The potentially avoidable tragedy of Bhopal has also forced us to consider global questions of corporate responsibility, relationships between governments and corporations, and the complex socio-cultural factors involved in the transfer of sophisticated technologies from industrialized countries to Third-World countries.

Multinational corporations have an important and constructive role to play in promoting economic growth and environmental protection in the Third World. This proves to be difficult in practice, however, given the various and often inconsistent cultural value systems and legal structures that exist between different nations. Nevertheless, one lesson from the Bhopal disaster is clear:

> If multinational corporations want access to markets and materials in developing countries, and if these countries want the benefit of direct foreign investment on a sustainable basis, then the public and private sectors will have to set new precedents in cooperating to achieve environmental protection. Unless this happens, further tragedies like Bhopal and other smaller and less visible incidents . . . will eat away the fabric of confidence on which progress depends. (Speth, 1988: 15)

One of the lessons to be learned from the Bhopal case is that the cause of technological disasters may involve factors that transcend organizational boundaries, such as social, political, and cultural variables. Kapitza (1993) identifies related kinds of socio-cultural causes involved in the failure at Chernobyl such as negligent regulation by the Soviet government of its commercial nuclear power industry. Valerii Legasov, chief deputy director of the Kurchatov nuclear energy institute, criticized Chernobyl management for not being more concerned with problems of safety in the overall operations of the plant (Rich, 1988: 285).

Neither the executive branch of the federal government nor the legislative, administrative, or judicial branches are adequately equipped with the knowledge and resources required to handle complex questions about the development and deployment of large-scale sociotechnical systems. This is one significant lesson

John Kemeny, Chairman of the Kemeny Commission on Three Mile Island, draws from the accident at Three Mile Island:

> The message I want to give you, after a hard and long reflection, is that I'm very much afraid it is no longer possible to muddle through. The issues we deal with do not lend themselves to that kind of treatment alone. Therefore, I conclude that our democracy must grow up. (Kemeny, 1980: 74)

Kemeny has two suggestions for democracy's maturity in an age of technology. First is "the existence of respected, nonpartisan, interdisciplinary teams" of specialists involved at all levels of public policy concerning decision making about technology (Kemeny, 1980: 74). Kemeny's second suggestion emphasizes the proper training and education of scientists and technologists, an education that goes beyond the simple dissemination of technical facts and mathematical theories. There is a need to "educate the next generation of leaders so that they can directly understand and come to grips with the monumental issues of our time" (Kemeny, 1980: 74). Kemeny's main lessons are reserved for technologists and politicians. These two groups, along with corporations, are primarily responsible for the development and deployment of potentially hazardous technologies.

Who is responsible for safeguarding the public's interests when dangerous technologies are developed and implemented? Included among relevant watchdog organizations are government agencies and public interest groups, along with various professional societies responsible for setting safety standards. There are indeed a variety of government agencies with a mandate to protect the public against harms produced by different industries. The same can be said for professional and educational organizations. However, the diffusion of responsibility among the multiple organizations all too often results in the actual neglect of the social and economic harms caused by failures of technology.

As we will see in Part V, where we take up these policy issues in more detail, the present state of our educational, professional, and political institutions reveals that serious hurdles must be overcome in order to protect ourselves from technological hazards.

In sum, failures of technology teach us about the limitations of human knowledge, the tragedy of hubris, the complacency with which we treat the powers of technology, and the failure of our institutions to control and manage individual and societal risks. "We cannot allow our fascination with the power of what we can do to blind us to what we cannot. It is no longer a matter of humility. It is a matter of survival" (Dumas, 1999: 328).

Understanding gained from a close analysis of technological disasters, suggests the identification of a set of general lessons—such as those listed in Figure 9-4—which, if heeded, could lead to the design, development, and management of safer and more reliable technology.

1. Despite expert engineering design and the application of "state-of-the-art knowledge," there is no total immunity from risk. A frequent disjuncture between science and technology increases the probability of failure.
2. No matter how sophisticated the hardware, the human element is present in setting requirements, setting designs to meet them, in production, testing, installation, maintenance, repair, and operation. Moreover, human beings are vulnerable to ignorance, error, and greed.
3. Malfunctions due to human error, especially in decision making, are more likely when psychological factors such as stress, anxiety, or "groupthink" are operative.
4. Organizational complexity places special demands on communication linkages that are often inadequate, fragmented, and nonintegrated.
5. The routine management of technology is too often focused on narrow organizational objectives that seek to maintain the status quo, meet deadlines and quotas, and reduce costs. Such objectives tend to compromise the safety of technological systems.
6. In almost all of the cases discussed, failure to properly assess the potential negative impact of technology consequently led to the resulting tragic effects.
7. Technology acts as an organizing force that requires massive natural, human, and financial resources, all of which have the tendency to concentrate both economic and political power in the hands of the few people who control it, often at the expense of vulnerable groups in society.
8. Complex technologies are supposedly monitored and controlled by public policy implemented at the governmental level. These policies are intended to safeguard both people and property. However, both administrative agencies, and citizen "watchdog" groups are often bureaucratized and/or underfunded, rendering them unable to achieve their objectives.
9. It is crucial that communication between the private and public sectors be made visible and publicly accountable. This would lead to more democratic governance over decisions regarding technological development.
10. Every failure of technology raises ethical issues because society is technology's ultimate patron and is thus affected by all of technology's impacts and consequences.

Figure 9-4
General lessons learned from the analysis of case studies of technological disasters.

Conclusion

The case studies presented throughout this book have drawn attention to the various engineering, economic, organizational, political, and cultural constraints that impede effective learning from the lessons provided by technological disasters. Due to such constraints, learning is all too often incremental and unsystematic rather than comprehensive and systematic. Would that Petroski's observations were true that "the more case histories a designer is familiar with or the more general the lessons he or she can draw from the cases, the more likely the patterns of erroneous thinking can be recognized and generalizations reached about what to avoid" (Petroski, 1994: 6). Current learning from technological disasters can be best characterized as "muddling through" (Lindblom, 1957). However, muddling through is inadequate in that it fails to lead to a "paradigm shift" in organizational, institutional, and social learning essential for the kind of collective wisdom needed for the design, development, and diffusion of safer, more reliable, and more humane technologies. The set of general lessons enumerated in Figure 9–4 attempt to provide the first steps toward such a systematic paradigm shift.

References

Anonymous. (1998). "Ukraine tallies sharp rise in illnesses near Chernobyl," *The New York Times,* April 23: A5.

Dumas, Lloyd. (1999). *Lethal arrogance: Human fallibility and dangerous technologies.* New York: St. Martin's Press.

Glegg, Gordon L. (1971). *The design of design.* Cambridge, England: Cambridge University Press.

Houlder, V. (2000). "Hole in ozone layer could be closed within 50 years," *Financial Times,* December 4: 16.

Jasanoff, Sheila. (1991). "Introduction: Learning from disaster." In *Learning from disaster: Risk management after Bhopal.* Philadelphia: University of Pennsylvania Press: 1–21.

Kapitza, Sergei. (1993). "Lessons of Chernobyl: The cultural causes of the meltdown," *Foreign Affairs* 72 (3): 7–12.

Kemeny, John G. (1980). "Saving American democracy: The lessons of Three Mile Island," *Technology Review* 83 (7): 65–75.

Kerkin, A. (2000). "Treaty talks fail to find consensus in global warming," *The New York Times,* November 26: 1.

Lindblom, Charles. (1957). "The science of muddling through," *Public Administration Review* 19: 79–88.

Mark, Hans. (1987). "The Challenger and Chernobyl: Lessons and reflections." In Hans Mark, Tom L. Beauchamp, Jesse Luton, Martin Marty, and Andrew Cecil (Eds.), *Traditional moral values in the age of technology.* Dallas: University of Texas Press: 31–57.

Martin, M., and Schinzinger, R. (1996). *Ethics in engineering.* New York: McGraw-Hill.

Peterson, Russell W. (1982). "Three Mile Island: Lessons learned for America." In Christoph Hohenemser and Jeanne X. Kasperson (Eds.), *Risk in the technological society.* Boulder, CO: Westview Press: 35–45.

Petroski, Henry. (1985). *To engineer is human: The role of failure in successful design.* New York: St. Martin's Press.

Petroski, Henry. (1994). *Design paradigms: Case histories in error and judgment in engineering.* Cambridge, England: Cambridge University Press.

Rich, Vera. (1988). "Legasov's indictment of Chernobyl managment," *Nature,* 333 (26): 285.

Roush, Wade. (1993). "Learning from technological disasters," *Technology Review,* August/September: 50–58.

Sethi, Praskash S. (1992). "The inhuman error: Lessons from Bhopal," *New Management* 8: 40–46.

Speth, James. (1988). "What we can learn from Bhopal," *Environment* 27 (1): 15.

Tenner, Edward. (1997). *Why things bite back: Technology and the revenge of unintended consequences.* New York: Vintage Books.

Van Duyne, S. (1994). "Apollo I capsule fire." In N. Schlager (Ed.), *When technology fails: Significant technological disasters, accidents, and failures of the twentieth century.* Detroit, MI: Gale Research: 580–586.

Wexler, Mark. (1990). "Learning from Bhopal," *The Midwest Quarterly* (31): 106–129.