Design Concepts for Engineers

Fifth Edition

MARK N. HORENSTEIN
Department of Electrical and Computer Engineering
Boston University

PEARSON

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

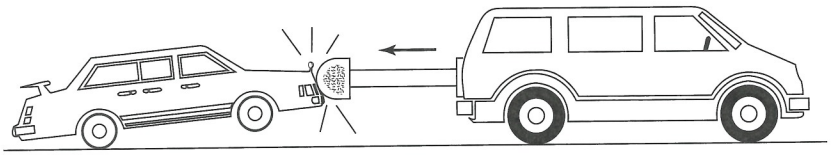


Figure 6.2
More realistic battering ram design as an offensive strategy.

paper and also on a CAD program, the arm failed miserably when mounted on the car. When an opposing vehicle was lifted into the air, the center of gravity fell outside the maximum allowed wheelbase of the vehicle, causing *both* vehicles to topple over and fall off the track. The students had to abandon their arm design and eventually settled on the battering ram shown in Figure 6.2 for their offensive strategy.

6.3 THE ROLE OF FAILURE IN ENGINEERING DESIGN: CASE STUDIES

The pages of engineering history are full of examples of design flaws that escaped detection in the design phase only to reveal themselves once the device was in use. Although many devices are plagued by minor design flaws from time to time, a few failure cases have become notorious because they affected many people, caused great property damage and fatalities, or led to sweeping changes in engineering practice. In this section, we review several classic design failures from the annals of engineering lore. Each event involved the loss of human life or major destruction of property, and each was caused by an engineering design failure. The mistakes were made by engineers who did the best they could, but had little prior experience or had major lapses in engineering judgment. After each incident, similar disasters were averted, because engineers were able to study the *causes* of the problems and establish new or revised engineering **standards** and guidelines. Studying these classic failures and the mistakes of the engineers who caused them will help you to avoid making similar mistakes in your own work.

The examples of failure that follow all had dire consequences. Each occurred once the product was in use, long after the initial design, test, and evaluation phases. Remember that it's always better for problems to show up *before* the product has gone to market. Design problems can be corrected easily during testing, burn-in, and system evaluation. If a design **flaw** shows up in a product or system that has already been delivered for use, the consequences are far more serious. As you read the examples of this section, you might conclude that the causes of these failures in the field should have been obvious, and that their occurrences were the result of some engineer's carelessness. Indeed, it's relatively easy to play "Monday-morning quarterback" and analyze the cause of a failure *after* it has occurred. But as any experienced engineer will tell you, spotting a hidden flaw during the test phase is not always easy when a device or system is complex and has many parts or subsystems that interact in complicated ways. Even simple devices can be prone to hidden design flaws that elude the test and evaluation stages. One of the marks of a good engineer is the ability to ferret out flaws and errors *before* the product finds its way to the end user. You can help to strengthen your intuition at flaw detection by becoming familiar with the classic failure incidents discussed in this section. If you are interested in learning more details about any of the case studies, you might consult one of the references listed at the end of the chapter.

6.3.1 Case 1: Tacoma Narrows Bridge

The Tacoma Narrows Bridge, built across Puget Sound in Tacoma, Washington in 1940, was the longest suspension bridge of its day. The design engineers copied the structure of smaller, existing suspension bridges and simply built a longer one. As had been done with countless shorter spans, support trusses deep in the structure of the bridge's framework were omitted to make it more graceful and visually appealing. No calculations were done to prove the structural integrity of a longer bridge lacking internal support trusses. Because the tried-and-true design methods used on shorter spans had been well tested, the engineers assumed that these design methods would work on longer spans. However, they were incorrect. On November 7, 1940, during a particularly windy day, the bridge started to undulate and twist, entering into the magnificent torsional motion shown in Figure 6.3. After several hours, the bridge crumbled as if it were made from dry clay; not a single piece of the bridge remained between the two main center spans.

What went wrong? The engineers responsible for building the bridge had relied on calculations made for smaller bridges, even though the assumptions behind those calculations did not apply to the longer span of the Tacoma Narrows Bridge. Had the engineers heeded some basic scientific intuition, they would have realized that three-dimensional structures cannot be directly scaled upward without limits.

6.3.2 Case 2: Hartford Civic Center

The Hartford Civic Center was the first of its kind. At the time of its construction in the mid-1970s, no similar building had ever been built. Its roof was made using a frame structure of interconnected trusses and joints, (Figure 6.4) rather than from a more conventional I-beam construction method. Hundreds of rods were interconnected in a visually appealing, two-layer pattern consisting of an array of horizontal steel bars and diagonal interconnects. Instead of performing detailed hand calculations, the design engineers relied on the latest computer models to compute the loading on each individual member of the roof structure. Recall that computers

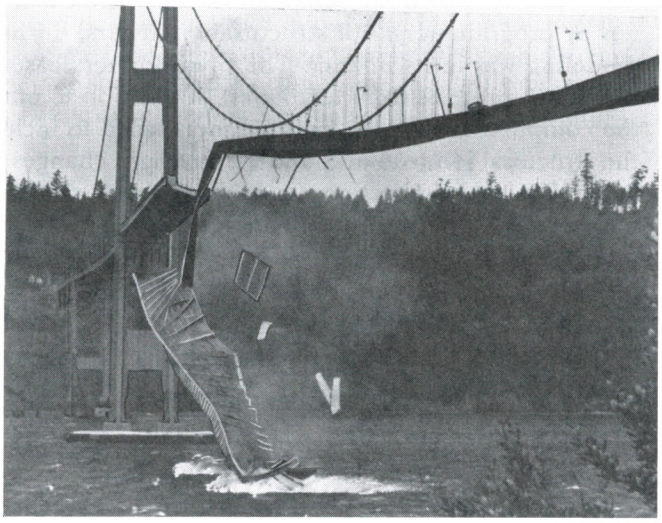


Figure 6.3
The Tacoma Narrows Bridge in torsional vibration.
(Photo courtesy of the US Bureau of Land Reclamation)

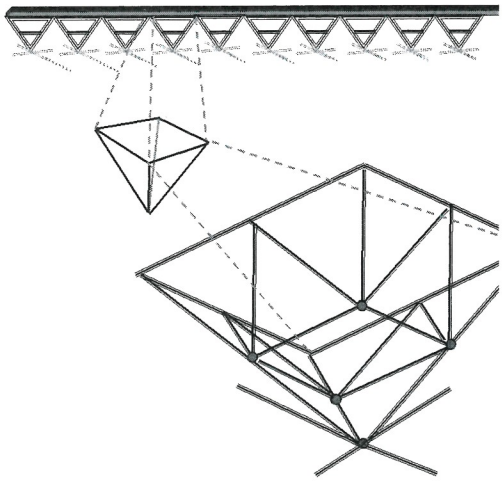


Figure 6.4
Truss and joint structure, consisting of arrays of horizontal bars and diagonal interconnects, designed to hold up the Hartford Civic Center roof.

in those days were much more primitive than those we enjoy today. The PC had not yet been invented, and all work was performed on mainframe computers that were very slow by today's standards. Hence the engineers used a simplified computational model that ignored susceptibility of the structure to torsional buckling modes. It was this mode of failure that initiated the collapse of the Civic Center roof, but the deficiency in the design was left undetected by the computer simulations.

On January 18, 1978, just a few hours after the center had been filled to capacity with thousands of people watching a basketball game, the roof collapsed under a heavy snow load, demolishing the building. Miraculously, no one was hurt in the collapse.

Why did the collapse occur? Some attribute the failure to the engineers who designed the civic center and chose not to rely on their basic judgment and intuition gleaned from years of construction practice. An investigation after the collapse revealed that field engineers noticed anomalies in the structure during its assembly and erection, but their concerns were not heeded by the project managers who chose to rely on the computer models. These computer models had been written by programmers, not structural engineers, during the days when computer modeling was in its infancy. The programmers based their code algorithms on structural formulas from textbooks. In addition to omitting buckling modes from the computer model, the programmers failed to include basic derating factors at the structural joints to account for the slight changes in layout (e.g., variations in angles, lengths, connections, and fabrication methods) that occur when a complex structure is actually built. The design engineers trusted the output of computer models that had never been fully tested. Under a normal roof load, many of the truss joints were stressed beyond their safe limits. The addition of a heavy snow load proved too much for the structure to bear.

6.3.3 Case 3: Space Shuttle Challenger

The NASA Space Shuttle *Challenger* blew up during launch on a cold day in January 1986 at Cape Kennedy (Canaveral) in Florida. Thousands witnessed the explosion in real time on live television (Figure 6.5). Hundreds of millions watched news

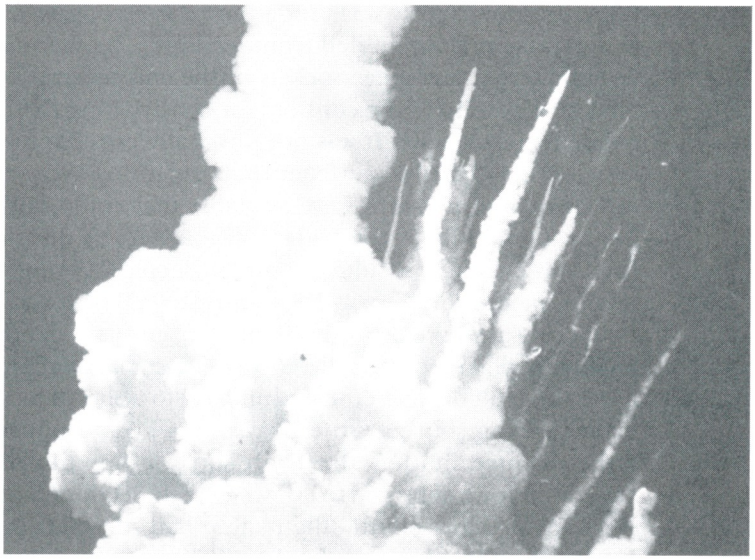


Figure 6.5
The Space Shuttle *Challenger* explodes during launch.
(Photo courtesy of NASA)

tapes of the event for weeks afterward. After months of investigation, NASA traced the problem to a set of O-rings used to seal sections of the multisegmented booster rockets. The seals were never designed to be used in cold weather, and on that particular day, it was about 28°F (−2°C) a very cold day for Florida. The overly cold O-rings either were too stiff to properly seal the sections of the booster rocket or became brittle and cracked due to the unusually cold temperatures. Flames spewed from an open seal during acceleration and ignited an adjacent fuel tank. The entire spacecraft blew up, killing all seven astronauts on board, including a high school teacher. At the time, it was the worst space disaster in U.S. history.

In using O-rings to seal adjacent cylindrical surfaces, such as those depicted in Figure 6.6, the engineers had relied on a standard design technique for rockets. However, O-rings had never been used on a rocket as large as the *Challenger's* booster rockets. This factor, combined with the unusually cold temperature, brought the seal to its limit, and it failed.

There was, however, another dimension to the failure. *Why* had the booster been built in multiple sections, requiring O-rings in the first place? The answer is complex, but the cause was largely attributable to one factor: The decision to build a multisection booster was, in part, *political.* Had engineering common sense been the sole factor, the boosters would have been built in one piece without O-rings.

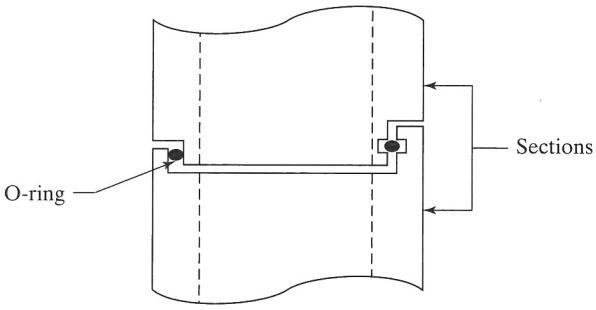


Figure 6.6
Schematic depiction of O-ring seals.

Joints are notoriously weak spots, and a solid body is almost always stronger than a comparable one assembled from sections. The manufacturing technology existed to build large, one-piece rockets of the correct size. But a senator from Utah lobbied heavily to have the contract for constructing the booster rockets awarded to a company in his state. It was not physically possible to transport a large, one-piece booster rocket all the way from Utah to Florida over existing rail lines. Trucks were too small, and no ships were available that could sail to land-locked Utah, which lies in the middle of the United States. NASA's decision to award the contract to the Utah company resulted in a multisection, O-ring-sealed booster rocket whose smaller pieces could easily be shipped by rail or truck.

Some say the catastrophe resulted from a lack of **ethics** on the part of the design engineers who suspected the O-ring design of having potential problems. Some say it was the fault of NASA for succumbing to political pressure from Congress, its ultimate funding source. Others say it was just an unusual convergence of circumstances, since neither the Utah senator nor the design engineers knowingly advocated for a substandard product. The sectioned booster had worked flawlessly on many previous shuttle flights that had not been launched in subfreezing temperatures. Still, others say that by putting more weight on a political element of the project, rather than on pure engineering concerns, the engineers were compromised into a less-than-desirable design concept that had never before been attempted on something so large.

6.3.4 Case 4: Kansas City Hyatt

If you've ever been inside a Hyatt hotel, you know that their internal architectures are unique. The typical Hyatt hotel has cantilevered floors that form an inner trapezoidal atrium, and the walkways and halls are open, inviting structures. In the case of the Kansas City Hyatt, first opened in 1981, the design included a two-layer, open-air walkway that spanned the entire lobby in midair, from one balcony to another. During a party that took place not long after the hotel opened, the walkway was filled with people dancing in time to the music. The weight and rhythm of the load of people, perhaps in resonance with the walkway, caused it to collapse suddenly. Over one hundred people died, and the event will be remembered forever in the history of hotel management. Although the hotel eventually reopened, to this day the walkway has never been rebuilt.

The collapse of the Hyatt walkway is a classic example of failure due to lack of construction experience. In this case, however, the error originated during the *design* phase, not the construction phase. In order to explain how the walkway collapsed, consider the sketch of the skeletal frame of the walkway, as specified by the design engineer, shown here in Figure 6.7.

Each box beam was to be supported by a separate nut threaded onto a suspended steel rod. The rated load for each nut-to-beam joint was intended to be above the maximum weight encountered during the time of the accident. What's wrong with this picture? The problem is that the specified structure was not realistic to build. The design called for the walkway's two decks to be hung from the ceiling by a single rod at each support point. The rods were made from smooth steel with no threads. Threading reduces the diameter of a rod, so it's impossible to get a nut to the middle of a rod unless the rod is threaded for at least half its length. To construct the walkway as specified, each rod would have to be threaded for 20 feet, and numerous rods were needed for the long span of the walkway. Even with an electric threading machine, it would have taken days to thread all the needed rods. The

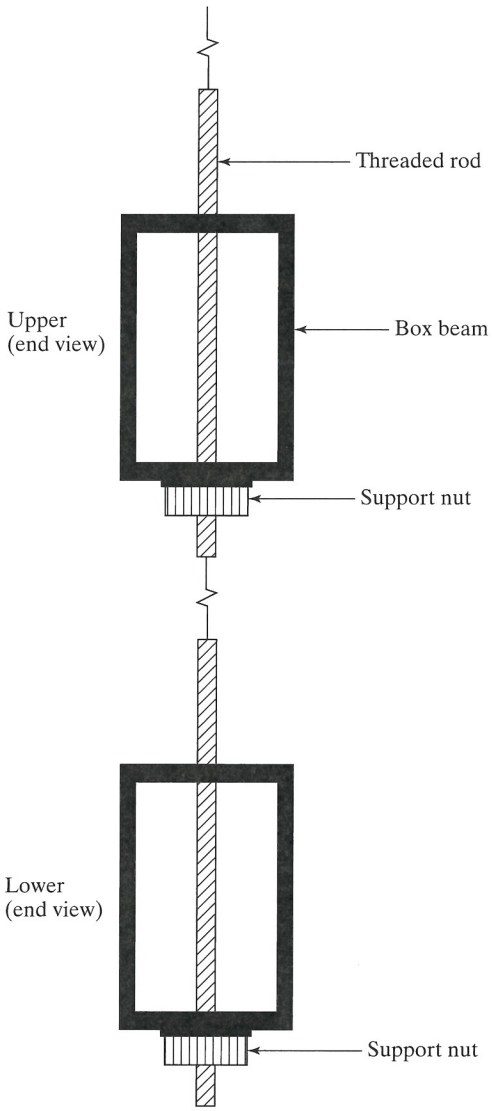


Figure 6.7
Kansas City Hyatt walkway support structure as designed.

contractor who actually built the walkway proposed a modification to the construction so that only the very ends of the rods would have to be threaded. The modification is illustrated in Figure 6.8.

The problem with this modification is that the nut (A), which was located at the lower end of the upper rod, now had to support the weight of *both* walkways. As an analogy, consider two mountain climbers hanging onto a rope. If both grabbed the rope simultaneously, but independently, their individual grips could hold their weights. If the lower climber instead grabbed the ankles of the upper climber, however, the upper climber's hands would have to hold the weight of *two* climbers. Under the full, or maybe excessive, load conditions of that day, the weight on nut (A) of the Hyatt walkway was just too much, and the joint gave way. Once the joint on one rod failed, the complete collapse of the rest of the joints and the entire walkway quickly followed.

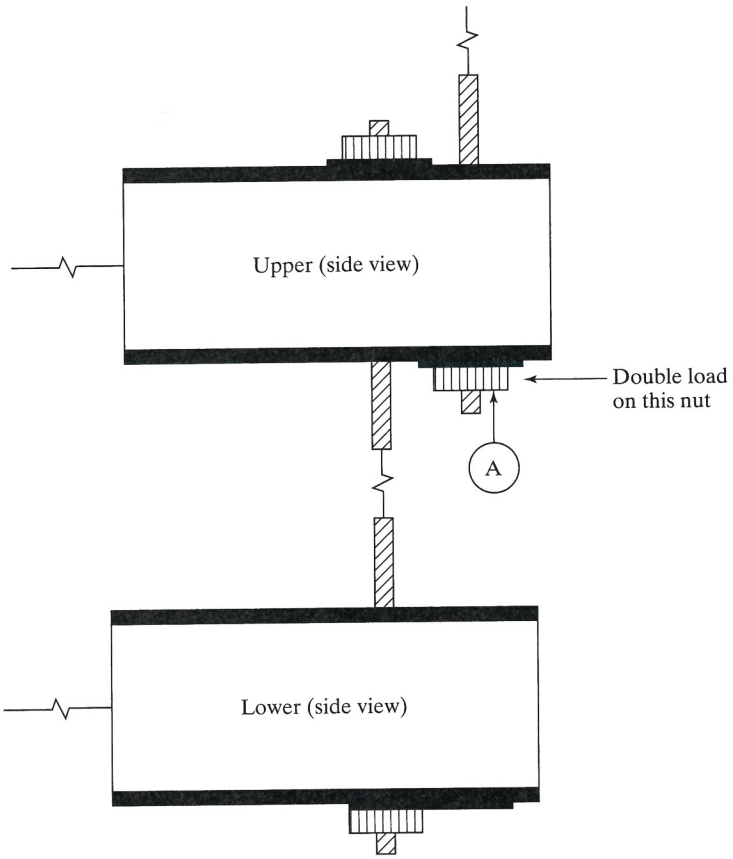


Figure 6.8
Kansas City Hyatt walkway support structure as actually built.

Some attributed the fatal flaw to the senior design engineer who specified single rods requiring 20 feet of threading. Others blamed it on the junior engineer, who signed off on the modifications presented by the construction crew at the construction site, and the senior engineer, who should have communicated to the junior engineer the critical nature of the rod structure as specified. Perhaps both engineers lacked seasoning—the process of getting their hands dirty on real construction problems to understand how things are made in the real world.

Regardless of who was at fault, the design also left little room for **safety margins**. It's common practice in structural design to leave *at least* a factor-of-two safety margin between the calculated maximum load and the expected maximum load on a structure. The safety margin allows for inaccuracies in load calculations due to approximation, random variations in material strengths, and small errors in fabrication. Had the walkway included this common safety margin, the doubly stressed joint on the walkway might not have collapsed, even given its modified construction. The design engineers specified a walkway structure that was possible, but not practical, to build. The construction supervisor was unaware of the structural implications, but was eager to complete the job. Hence he ordered a seemingly innocent, but ultimately fatal, change in the construction method. If either of the design engineers had had more experience working on a construction site, this shortcoming might have been discovered. Errors such as the Kansas City Hyatt's walkway collapse can be prevented by including workers from all phases of construction in the design process, ensuring adequate communication between all

levels of employees, and adding far more than minimal safety margins where public safety is at risk.

6.3.5 Case 5: Three Mile Island

Three Mile Island was a large nuclear power plant in Pennsylvania (see Figure 6.9). It was the site of the worst nuclear accident in the United States, and it was nearly comparable to the total meltdown at Chernobyl, Ukraine. Fortunately, the incident at Three Mile Island resulted in only a near miss at a meltdown. However, it also led to the shut-down and trashing of a billion-dollar electric power plant, resulting in significant loss of electrical generation capacity to the power grid in the eastern United States.

On the day of the accident, a pressure buildup occurred inside the reactor vessel. In such situations, it was normal procedure to open a relief valve to reduce the pressure to safe levels. The valve in question was held closed by a spring and was opened by applying voltage to an electromagnetic actuator. However, the designer of the electrical control system had made one critical mistake. As suggested by the schematic diagram in Figure 6.10, indicator lights in the control room lit up when power was applied to or removed from the valve actuator coil. Unfortunately, the control panel gave no indication about the *actual* position of the valve. After the pressure-relief operation, the valve at Three Mile Island became stuck in the open position. Although the actuation voltage had been turned off and lights in the control room indicated that the valve was closed, it was actually stuck open.

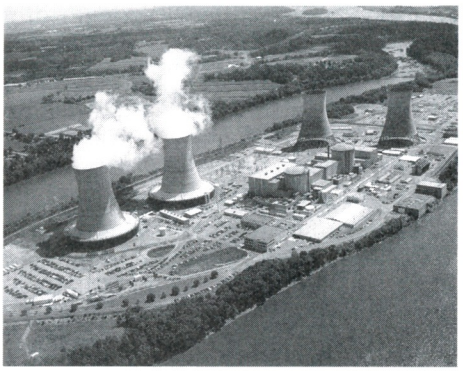


Figure 6.9
Three Mile Island power plant.
(Photo courtesy of the US Dept of Energy)

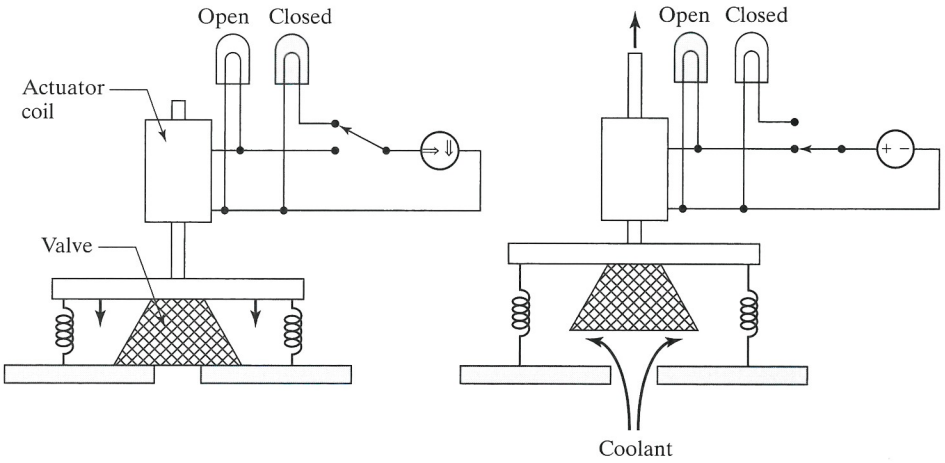


Figure 6.10
Valve indicator system as actually designed.

The mechanical spring responsible for closing the valve did not have enough force to overcome the sticking force. The operators, believing that the valve was closed, tried to diagnose the problem; meanwhile, coolant leaked from the vessel for almost two hours. Had the operators known that the valve was open, they could have closed it manually or taken other corrective measures. In the panic that followed, however, the operators continually believed their control-panel indicator lights and thought that the valve was closed. Eventually, the problem was contained, but not before a rupture nearly occurred in the vessel. Such an event would have resulted in a complete core meltdown and spewed radioactive gas into the atmosphere. Even so, damage to the reactor core was so severe that the plant was permanently shut down. It has never reopened.

The valve actuation system at Three Mile Island was designed with a poor human–machine interface. The ultimate test of such a system, of course, occurs during an emergency, when the need for absolutely accurate information is critical. The operators assumed that the information they were receiving was accurate, while in reality it was not. The power plant's control panel provided the key information by inference, rather than by direct confirmation. A better design would have included an independent sensor that unambiguously verified the true position of the valve, as suggested by the diagram of Figure 6.11.

6.3.6 Case 6: USS Vincennes

The *Vincennes* (Figure 6.12) was a U.S. missile cruiser stationed in the Persian Gulf during the Iran–Iraq war. On July 3, 1988, while patrolling the Persian Gulf, the *Vincennes* received two IFF (Identification: Friend or Foe) signals on its Aegis air-defense system. Aegis was the Navy's complex, billion-dollar, state-of-the-art information-processing system that displayed more information than any one operator could possibly hope to digest. Information saturation was common among operators of the Aegis system. The *Vincennes* had received two IFF signals, one for a civilian plane and the other for a military plane. Under the pressure of anticipating a possible attack, the overstimulated operator misread the cluttered radar display and concluded that only one airplane was approaching the *Vincennes*. Repeated attempts to reach the nonexistent warplane by radio failed. The captain concluded that his ship was under attack and made the split-second decision to have the civilian airplane shot down. Two hundred ninety civilians died needlessly.

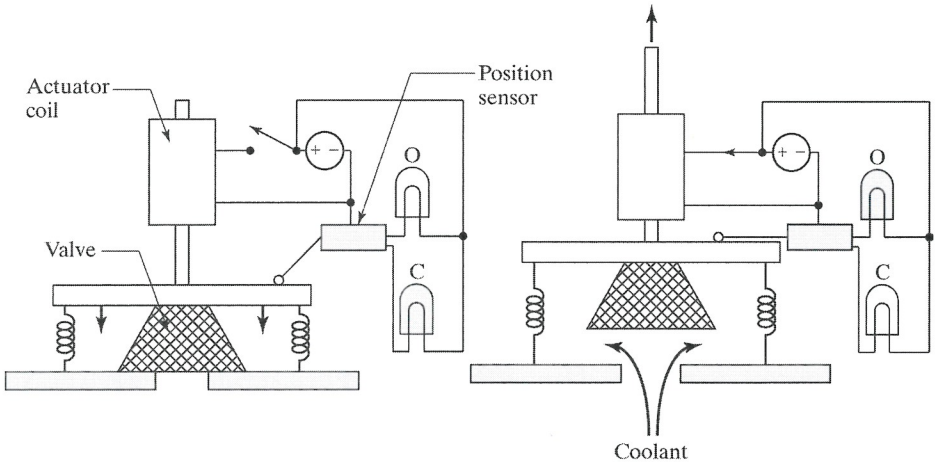


Figure 6.11
Valve indicator system as it should have been designed and built.

Figure 6.12
The USS Vincennes.
(Photo courtesy of the National Park Service)

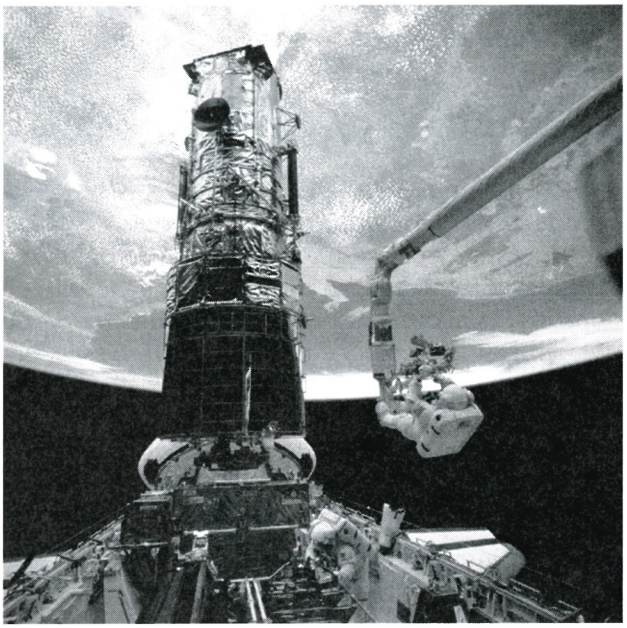
What caused this catastrophic outcome? Was it bad military judgment? Was it an operating error? Were the engineers who designed the system at fault? The Navy officially attributed the accident to "operator error" by an enlisted sailor, but in some circles the blame was placed on the engineers who had designed the system. Under the stress of possible attack, and deluged with information, the operator simply could not cope with an ill-conceived human–machine interface. Critical information, which is needed most during crises, should have been uncluttered and easy to interpret. The complex display of the Aegis system was an example of something that was designed just because it was technically possible. It resulted in a human–machine interface that became a weak link in the system.

6.3.7 Case 7: Hubble Telescope

The orbiting Hubble telescope was put into space at a cost of over a billion dollars. Unaffected by the distortion experienced by ground-based telescopes due to atmospheric turbulence, the Hubble has provided spectacular photos of space and has made possible numerous astronomical discoveries. Yet the Hubble telescope did not escape design flaws. Of the many problems that plagued the Hubble during its first few years, the most famous was its improperly fabricated mirrors. They were distorted and had to be corrected by the installation of an adaptive optical mirror that compensated for aberrations. The repairs were conducted by a NASA Space Shuttle crew. Although this particular flaw is the one most often associated with the Hubble, it was attributed to sloppy mirror fabrication rather than to a design error.

Another little-known design error more closely illustrates the lessons of this chapter. The Hubble's solar panels were deployed in the environment of space, where they were subjected to alternate heating and cooling as the telescope moved in and out of the Earth's shadow. The resulting expansion and contraction cycles caused the solar panels to flap like the wings of a bird. Attempts to compensate for the unexpected motion by the spacecraft's computer-controlled stabilizing program led to a positive feedback effect, which only made the problem worse. Had the design engineers anticipated the environment in which the telescope was to be operated, they could have compensated for the heating and cooling cycles and avoided the problem. This example illustrates that it's difficult to anticipate all the conditions under which a device or system may be operated. Nevertheless, extremes

in operating environment often are responsible for engineering failures. Engineers must compensate for this problem by testing and *retesting* devices under different temperatures, load conditions, operating environments, and weather conditions. Whenever possible (though obviously it was not possible in the case of the Hubble), a system should be tested in as many different environmental conditions as possible, particularly if those conditions may be encountered in the field.



(Photo courtesy of NASA)

6.3.8 Case 8: de Havilland Comet

The de Havilland Comet was the first commercial passenger jet aircraft. A British design, the Comet enjoyed many months of trouble-free flying in the 1950s until several went down in unexplained crashes. Investigations suggested that the fuselages of these planes had ripped apart in midflight. For years, the engineers assigned the task of determining the cause of the crashes were baffled. What, short of an explosion, could have caused the fuselage of an aircraft to blow apart in flight? No evidence of sabotage was found at any of the wreckage sites. After some time, the cause of the crashes was discovered. No one had foreseen the effects of the numerous pressurization and depressurization cycles that were an inevitable consequence of takeoffs and landings. Before jet aircraft, lower altitude airplanes were not routinely operated under pressure. Higher altitude jet travel brought with it the need to pressurize the cabin. In the case of the Comet, the locations of the window rivets developed fatigue cracks; after many pressurization and depressurization cycles, the fatigue cracks grew into large, full-blown cracks in the fuselage. This mode of failure is depicted in Figure 6.13.

Had the design engineers thought about the environment under which the finished product would be used, the problem could have been avoided. Content instead with laboratory stress tests that did not mimic the actual pressurization and

depressurization cycles, the engineers were lulled into a false sense of security about the soundness of their design. This example of failure again underscores an important engineering lesson: Always test a design under the most realistic conditions possible. Always assume that environmental conditions will affect performance and reliability.

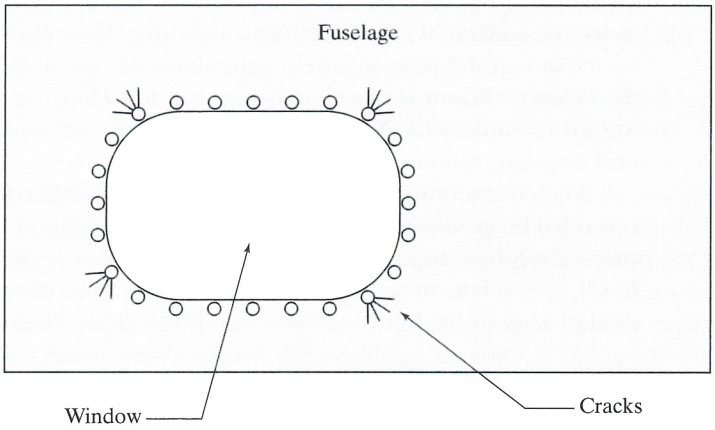


Figure 6.13
Stress cracks around the window rivets of the de Havilland Comet.

6.3.9 Case 9: The Collapsing Roof Panels

On July 10, 2006, a man and woman were driving through one of Boston's famed "Big Dig" tunnels, a connector from US Interstate 90 to the Ted Williams Tunnel. Without warning, four concrete panel tiles, each weighing around three tons, fell from their ceiling mounts, crushing the car beneath. A total of about 26 tons of concrete and associated suspension hardware fell on the vehicle and the roadway. The man survived, but the woman was killed. (See Figure 6.14.)

For even the most novice of engineers, immediate questions come to the mind: How were these panels attached? Why were they made from concrete, and why so heavy? How could they have fallen so suddenly without prior signs of pending

Figure 6.14
Collapsed ceiling panels inside the "Big Dig."
(Photo courtesy National Transportation Safety Board)

failure? The answers to these questions are complex, but some very basic errors on the part of the designers, engineers, and installers unmask the breaches in ethical behavior, the pressures of economics, and the lure of monetary gain connected with this incident.

Boston, Massachusetts had a world-class traffic problem in the form of an elevated six-lane highway known as "The Central Artery." The roadway, built in the 1950s, cut through the heart of the city. When it opened in 1959, the Central Artery comfortably carried about 75,000 vehicles per day. By the 1980s, it was carrying more than 200,000 cars. The Central Artery/Tunnel Project, or "Big Dig," was conceived as a grand plan to ameliorate what were possibly the worst traffic problems in the country. When the project began in the 1980s, the projected cost through 2005 was an inconceivable $3.2 billion. By 2008, the accumulated costs for construction and ongoing repairs topped $21 billion.

The concrete Big Dig ceiling panels were designed to hang from the top of the tunnel. The panels were specified to be held by metal bracket supports attached to the ceiling by hanging rods. This configuration is illustrated in Figure 6.15. The holding brackets were to be anchored to the concrete ceiling via bolts inserted into drilled holes and held in place by epoxy glue. Thus the two-ton panels exerted

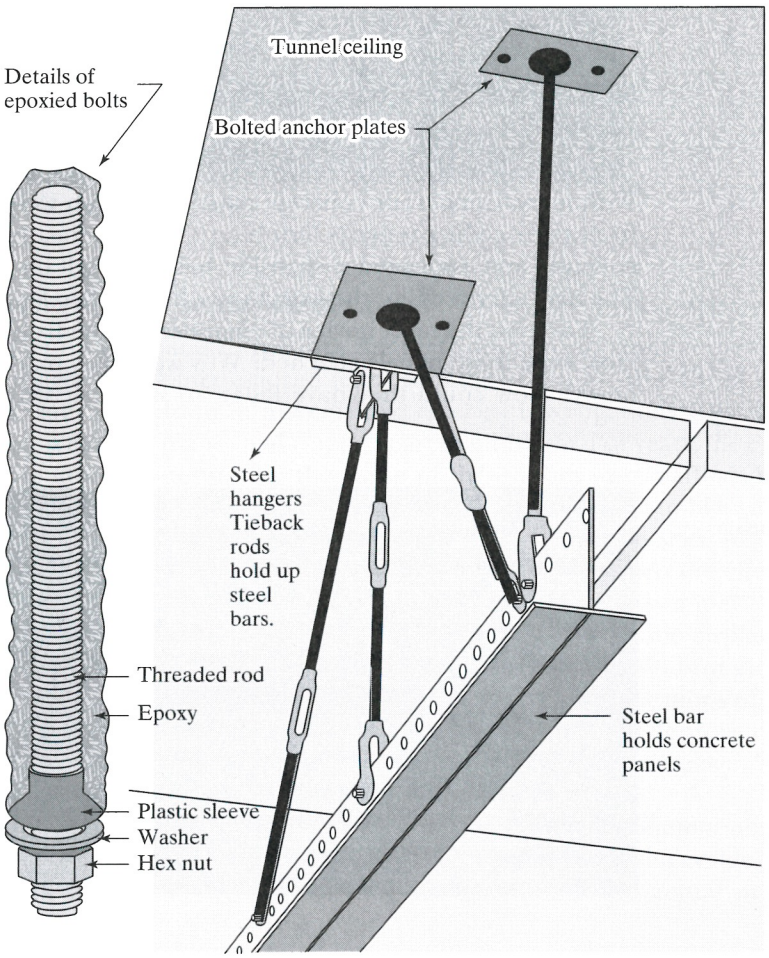


Figure 6.15
Details of support system for concrete ceiling panels. The upper brackets were secured by bolts inserted into holes drilled in the concrete ceiling. Epoxy glue filled the space between the bolts and the hole cavities.

constant axial (downward) force on the individual glued bolts installed in each vertically drilled hole.

Epoxy is a polymer whose stiffness changes with time and temperature. If a load is applied suddenly, the epoxy holds well for short periods. If the load is continuously applied thereafter (i.e., a "static load"), molecules in the polymer may begin to slide past one another, causing some epoxies to gradually deform in a process called "creep." The particular epoxy used in the tunnel had poor creep resistance. The fact was overlooked by the engineers responsible for installation. This lapse in rigor resulted from a general lack of understanding in the "construction community" about epoxy creep under static load.

To save time and materials, the main contractor used a fast set epoxy for installing the adhesive anchors into the ceiling. This epoxy formulation had been shown, via previous testing, to succumb to creep failure under sustained tensile loading.

The epoxy manufacturer neglected to inform the contractor about the lack of creep resistance of the specific epoxy being purchased for the job. Interestingly, bolts in other similarly anchored systems in earlier built sections of the Big Dig had shown signs of pulling out due to epoxy creep and were repaired.

Seven years before the accident, in 1999, a safety officer working for Modern Continental warned his superiors that the bolts could not possibly hold the heavy ceiling panels. The memo stated, in part, that he could not "comprehend how this structure can withhold the test of time."

The Massachusetts Turnpike Authority did not establish ongoing and timely inspection of tunnel components once the Big Dig was opened to traffic. Modern Continental similarly did not institute its own inspection program during and after construction to ensure that the installed ceiling anchors were working properly.

After investigating the ceiling panel disaster, the National Transportation Safety Board (NTSB) determined, not surprisingly, that the probable cause of the ceiling was the inappropriate use of an epoxy anchor adhesive that was not creep resistant. Over time, the epoxy deformed and fractured until several ceiling support anchors pulled free and allowed a portion of the ceiling to collapse.

As a result of its investigation, the NTSB issued new recommendations concerning the future use of tensile-loaded epoxies. One of those recommendations was to prohibit the use of adhesive anchors in sustained tensile-load overhead highway applications where failure of the adhesive would result in a risk to the public or, at the very least, to require creep testing on all anchor adhesives proposed for overhead applications. More importantly, countless generations of engineering students have studied this problem as a design exercise and have come up with numerous, simple mechanical modifications that would have prevented the accident.

6.3.10 Case 10: Citicorp Center

When the Citicorp Center was being planned in New York City in the late 1970s, the design engineers had a unique challenge. New York is by nature a crowded city, and a nearby structure, St. Peter's Lutheran Church, was situated on the northwest corner of Citicorp's desired building site. The owners of the church asked that, in exchange for use of that corner of the site, their building be torn down and rebuilt such that the Citicorp tower did not touch the new church structure.

The solution proposed by the engineer in charge of the project was to add giant columns set at the midpoint of each wall. This arrangement allowed each corner of the first nine floors of the new building to hover over the ground, with the

new church beneath one of them. This structural juxtaposition can be seen in Figure 6.16.

The engineer's design included crossed beams joined at the centers to allow the skyscraper to withstand high winds. The design also included a 400-ton actively tuned mass damper, run by electrical power, to help stabilize the building. In moving from the design phase to actual construction, however, the new building's owner skimped on the engineer's design requirements and substituted inexpensive, bolted joints for welds at the load-bearing beam crossings.

In 1978, an unknown undergraduate architecture student contacted the engineer with a bold claim: The Citicorp Center building could be toppled over by high winds. Normally, rectangular buildings are strongest at their corners, and the striking of winds at the faces causes the greatest strain. The student had been studying the Citicorp Center for an assignment and had found that the building was particularly vulnerable to winds striking at the corners. The design engineer had accounted for perpendicular winds but not so-called quartering winds. The engineer checked the student's calculations (which had been performed without the aid of modern computers) and found that, indeed, she was right. He compared the maximum sustainable winds for the new structure and determined from weather data that a storm strong enough to topple the Citicorp Center hits New York City about every 55 years. To make matters worse, the student's calculations assumed the tuned mass damper to be operating. In a major storm, a blackout could incapacitate the tuned mass damper. Without it, calculations and weather data predicted that a storm powerful enough to topple the building hits New York about every 16 years. In other words, during any given year, the Citicorp Center had a 1-in-16 chance of collapsing.

The redesign solution developed by the engineer required the building's structural joints to be reinforced by welding two-inch-thick steel plates over each of over 200 bolted cross braces. Work began immediately, in secret, and continued around the clock for three months. Carpenters worked during the day to expose the brace points from *inside* the walls of vacated offices. Welders worked all night installing the reinforcement plates. In case of imminent disaster due to an approaching storm, the city worked out a secret evacuation plan that was put in place for the surrounding area. The general public knew nothing of the circumstances, because the New York press was on strike at the time, hence news of the problem and the repairs was not widely disseminated. Once the reinforcements were finished, the entire structure was re-evaluated for safety and was found to be one of the most sturdiest skyscrapers in the world.

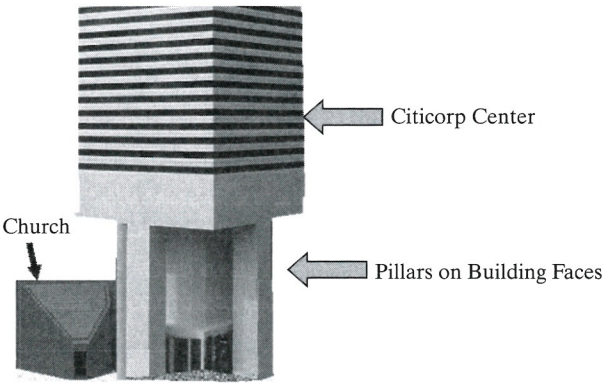


Figure 6.16
Citicorp tower. The Citicorp Center in New York City. The four support pillars are on the faces of the building, rather than on the sides.

The design for the Citicorp Center included a serious engineering flaw which went completely unnoticed during its construction and initial use. If this weakness had not been accidentally discovered by a diligent student, then secretly fixed, the tall skyscraper might have been toppled by a stiff gust of wind without any warning. Over forty years after the incident, the student has since been identified as Diane Hartley. She most certainly saved hundreds of lives and millions of dollars with her sharp eye and bold action.

6.3.11 Case 11: Ford Pinto

The internal combustion engine that propels most automobiles runs on gasoline, a highly combustible fluid stored in the underside of the vehicle. The auto industry has managed to keep fuel tank explosions rare, but fuel tank-related fires do occur. Arguably the most dangerous tank ever designed was the rear-mounted version installed in 1971 through 1976 models of the Ford Pinto.

The original design specifications for the Pinto were challenging. To keep it cost and fuel-efficiency competitive, it was to weigh no more than 2,000 lb (900 kg) and cost no more than $2,000 (in 1970 dollars). These requirements led to a fuel tank mounted behind the rear axle and in front of the rear bumper. Moreover, to save weight, the tank was not a self-integrated container. Rather, it consisted of a large, sheet-metal bottom pan welded to the underside of the car body, which served as the tank's upper surface (see Figure 6.17).

Well into the development of the Pinto, some engineers discovered that during low-speed, rear-end crash testing, the filler neck would tear away from the sheet-metal tank and spill fuel under the car. The tank could easily be punctured by the bolts that protruded from the rear-end differential gearbox and nearby mounting brackets. The puncturing could be so severe that all the fuel in the tank could leak out in less than a minute after an impact.

These problems constituted a serious fire risk. Proposed solutions included mounting an integral tank above the axle. Another was to install tank shields to prevent punctures, along with reinforcements around the filler to prevent tearing. Ford management performed a "cost–benefit analysis" and determined that fixing the known problems would increase the per-vehicle manufacturing cost by about $11, for an estimated total of $113 million over the production life of the car. The company, records show, weighed this added manufacturing cost against likely personal injury litigation for burns and future fatalities, estimated to be only $49 million.

By 1974, the National Highway Traffic Safety Administration (NHTSA) began investigating reports of failing fuel tank straps and fire incidents in the Pinto. These incidents eventually found their way into newspapers and other media. Several

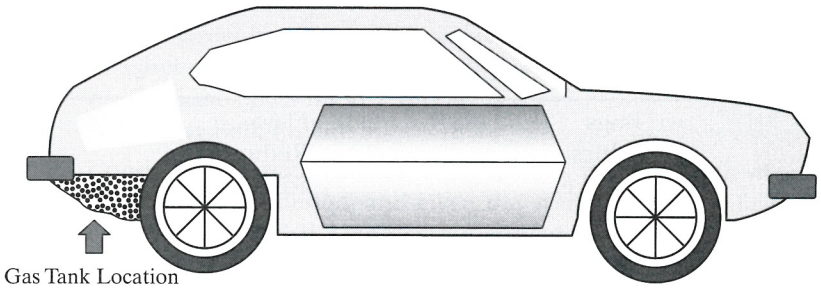


Figure 6.17
Ford Pinto. The Ford Pinto gas tank was located behind the rear axle of the vehicle.

Pinto-related litigations ensued. Given that the company knew about the problem, public outcry was such that, for example, a court in California awarded $125 million in damages (later reduced to $3.5 million) to an individual who had been injured in a low-speed accident when his Pinto burst into flames.

Eventually, by 1978, all affected Pintos were recalled and upgraded with the originally proposed shielding and reinforcements. In the years that followed, the fatality rate from rear-impact fuel tank fires was found to be about the same for vehicles made by Ford's competitors. The public relations damage had been done, however. The company gained a reputation for putting profits ahead of safety and quality, which took years to overcome. Ironically, perhaps because of this corporate lesson, Ford is now known to build some of the safest cars on the road.

6.4 PREPARING FOR FAILURE IN YOUR OWN DESIGN

First-time designs often betray previously hidden flaws after an initial period of successful use. Design flaws eventually show up because the operating environment changes, a previously untried sequence of events occurs, or weak points in the design encounter repeated stress. Sometimes, failure occurs just because of plain old statistics. As the saying goes, "If something is bound to fail, it *will* fail sooner or later." After a failure occurs, it's the engineer's job to determine the cause, fix the problem, and begin tests again. At the same time, it's up to the design engineer to identify as many of the bugs and weaknesses as possible during the early phases of the design process. Thorough testing and retesting under all sorts of operating conditions is essential. An unsuccessful first prototype presents an excellent opportunity to discover and weed out bugs before the final version of the device is put to market.

In the commercial sector, the rush to market a product ahead of competitors puts pressure on the engineer to complete the test and evaluation phases as quickly as possible. For this reason, many consumer products develop problems soon after they are released. If you purchase a product during its first year of issue, expect to find bugs and weaknesses that were not discovered on the factory floor.

Despite this admonition, you should be eager to apply your engineering design skills to new technology and innovation. If all engineers were content to stay with tried-and-true designs, technical progress would cease. Understanding when to stay within the bounds of a traditional design and when to move on to new creative frontiers requires experience, knowledge, and intuition. When you encounter failure in your own design projects, do not be discouraged. Recognize failure as an inevitable part of the design process. Use it to learn, discover, and expand your capabilities as an engineer. Remember, "There are no freak accidents, only unexpected ones."

KEY TERMS

Bugs	Flaw	Society
Ethics	Redundancy	Standards
Failure	Safety margin	