Determining Negligence in Engineering Failures

Course No: LE2-012
Credit: 2 PDH

Mark Rossow, PhD, PE, Retired

Continuing Education and Development, Inc.

P: (877) 322-5800
info@cedengineering.com

1 Introduction

The purpose of the present paper is to identify conditions under which, when an engineering failure has occurred, the failure can be attributed to negligence. The paper begins with a discussion of the definition of "negligence" and the closely related notion of the "standard of care" expected of an engineer. Because the occurrence of serious accidents always brings up the issue of whether adequate safety precautions were taken, the relation between safety and risk is discussed. Since a serious accident also usually results in a failure investigation, the biases often present in such investigations are described, as are the use and misuse of investigation reports by persons who differ widely in their motives. Finally these concepts are illustrated with a description of five case studies of failures ranging from gross negligence to absolutely unforeseeable events.

2 Expected behavior of engineers and the safety, health and welfare of the public

In terms of the well-being and protection of the public, expectations for engineers are defined through laws, regulations and codes of ethics. Laws express these expectations through the concept of "negligence."

2.1 Negligence

State licensing boards, laws, and professional organizations typically offer a definition of negligence similar to the following: [1, 2, 3]

> Negligence in the practice of professional engineering means the failure to behave with the standard of care that a professional engineer of ordinary prudence would have exercised under the same circumstances. The behavior usually consists of actions, but can also consist of omissions when there is some duty to act.

In a trial, deciding what is the expected standard of care and whether or not it has been met is usually beyond the expertise of lay people without the assistance of expert witnesses, although some acts of negligence are so obvious that even non-engineers can judge. An example of obvious negligence would be a structural engineer who was hired to review structural plans but approved them without having even seen them. It should be stressed, though, that even when expert testimony is given at a trial, the question of whether negligence has occurred still is decided by the jury. Even though jury members may lack expertise in a technical subject, they still must make a judgment about whether an expert witness is credible, or, when experts disagree, about which expert to believe.

2.2 More on standard of care

An important factor in defining the standard of care required in a particular technological application is whether the technology involved is mature or immature. "Mature" technologies have well-established design rules codified in design manuals and even in legal codes. Many instances of the technology have been implemented and designers have a large body of experience—their own or other's—to draw upon. Because of this extensive experience with the technology, almost all possible failure modes have been identified, and techniques for avoiding them are known. Reinforced concrete used in bridge design is an example of a mature technology.

In contrast, immature technologies do not have well-established design rules; in fact, design rules may be developed as part of a project using the technology. Because designers have comparatively little experience to draw upon, much analysis and small-scale testing of components are required, and the probability is greater that not all failure modes have been identified. Many subjective judgments must be made about whether or not experiments and calculations have been sufficient. The project consists as much in determining the design rules as in actually following the rules to produce a final product. The Apollo project to place a man on the moon involved much immature technology.

The point in drawing this contrast between mature and immature technologies is that the "standard of care" and "ordinary prudence" expected are quite different for the different technologies—what indeed does "ordinary" mean when a new technology is applied for the first time? Any analysis of engineering failure must take this difference in maturity into account when judging if standard of care and ordinary prudence considerations have been met.

2.3 Codes of ethics

In addition to laws against negligence contained in governmental statutes, statements defining expected standards of ethical behavior are written in the codes of ethics of many engineering professional organizations. Typical statements are "Engineers shall hold paramount the safety, health and welfare of the public … and "Engineers shall recognize that the lives, safety, health and welfare of the general public are dependent upon engineering judgments, decisions, and practices incorporated into structures, machines, products, processes and devices." [4] These statements of what constitutes ethical behavior amount to saying "Don't be negligent." That is, according to the definition of negligence stated above, an engineer should exercise a standard of care that a professional engineer of ordinary prudence would exercise. Thus codes of ethics and the definition of negligence are equivalent, at least as far as safety of the public is concerned. Codes of ethics cover other topics in addition to public safety, however, such as duty to clients, fraud, and bribery.

3 Safety, risk, and uncertainty

When an accident happens and people are injured or killed, questions of safety and risk always arise. To answer these questions, it is important to be clear about what the terms, "safety" and "risk," mean.

3.1 Safety

The general public tends to believe that safety is a binary property: something is either safe or unsafe, and there is no state or condition in between. For example, expressions such as "life is infinitely valuable," "the risk of injury or death must be zero," and "failure is not a possibility" are commonly heard and are all based on the assumption that the probability of failure can be reduced to zero—that is, a "safe" condition can be achieved in the absolute, or binary sense. Many of these ideas are easily refuted. For instance, if life is infinitely valuable, no rational person would ever drive an automobile, since risking something infinitely valuable in a situation where fatal accidents occur would be irrational.

A more realistic definition of "safe" is needed. William Lowrance, in his book, *Of Acceptable Risk*, suggests [5, p.8]

> A thing is safe, if its risks are judged to be acceptable.

Lowrance then defines risk as "the probability and severity of harm to human health." Thus the risk associated with an event can be visualized as a point on a line measuring probability values from zero to one, and something is called safe or unsafe, depending on someone's subjective judgment of where "acceptable" lies on the line. Risk can be estimated by specialists knowledgeable in the relevant technical area, for example, automotive engineers specializing in crashworthiness. Safety, on the other hand, is determined by a subjective judgment about how much risk someone is willing to accept.

3.2 Uncertainty

Safety and risk have been defined in terms of the probability of failure and thus are based implicitly on frequency distributions. The idea of risk and safety calculated from frequency distributions can be useful in incorporating risk analysis into engineering design. In fact, such probabilistic design approaches are widely used in a number of industries, for example, aerospace, electronics, medical devices, nuclear power, and structural design, to name only a few. In terms of the definition of negligence in law, designers using these approaches would generally be thought to be using the "standard of care" expected of a "prudent person."

But probabilistic design is not quite the end of the story. In a book published in 1921, the economist Frank Knight made a distinction between "risk," which applied to situations where the outcome cannot be predicted but the odds can be calculated, and "uncertainty," where we do not have enough information even to calculate the odds, or worse, we do not even anticipate the manner in which failure could occur. [6]

Knight applied his ideas to investment decision-making in business, and they have been subjected to some criticism over the years. However, in the 2008 U. S. financial crisis, Knightian uncertainty provided a good model of what occurred. Hard-working and highly intelligent financial analysts, many with doctoral degrees in mathematics and physics, constructed complex mathematical models that predicted the risk of mortgage-backed securities. These models were based on historical rates of defaults on mortgages; they assessed "risk" in the sense that Knight used it. But then occurred a huge drop in real-estate prices coupled with widespread fraud in approval of mortgages loans to unqualified buyers ("liar loans") and fraud in the marketing of mortgage-backed securities. Investors realized that the analysts' risk assessments were inadequate, and conditions of Knightian uncertainty prevailed. Investors then abandoned the market for other than the safest of investments, such as government bonds, and the value of non-governmental securities dropped precipitously.

An example of Knightian uncertainty will be given in the Case Studies.

Knight's distinction between risk and uncertainty shows that there are several aspects to determining whether or not negligence—in particular, failure to exercise an appropriate standard of care—has occurred in an engineering failure. On the one hand, the failure may have occurred because the designers erred in calculating the risk. On the other hand, the failure may have occurred because of conditions of Knightian uncertainty—no one could have predicted the event that caused the failure; the required standard of care to prevent the event was unknown beforehand.

3.3 Act of God

Readers familiar with contract law might ask how Knightian uncertainty relates to the phrase "an act of God" that sometimes appears in contract language. The two concepts overlap somewhat but are not identical. The phrase "an act of God" in contract law refers to a significant event attributed exclusively to "natural phenomena whose effects could not be prevented by the exercise of reasonable care and foresight." [7] Knightian uncertainty is much broader, including acts of God but also acts of man and applies not only to destructive events occurring but also anticipated events *not* occurring.

4 Failure investigations

When an engineering failure results in serious injury or death, usually an investigation of the causes of the failure is conducted. Ideally the investigation should produce a report that is, in the words of the Foreword to the report on the crash of the Concorde jet, [8]

> … intended neither to apportion blame, nor to assess individual or collective responsibility. The sole objective is to draw lessons from [the] occurrence which may help to prevent future accidents or incidents.

Thus even when the engineers involved are found to be negligent, the investigation should focus on how to improve present practice by proposing ways of detecting negligence in advance of a possible tragedy.

4.1 Use of investigation results

Not everyone who reads the investigators' report, however, will share the noble aim of learning how to prevent future accidents. Injured persons, relatives of persons who died in the accident, plaintiff's lawyers, insurance companies, law-enforcement officials, politicians looking for publicity, and news media personnel will study the report to find out who they can blame. Large corporations are often convenient targets, because they have "deep pockets" (money to settle lawsuits), and many members of the public already view them with suspicion, based on examples

of bad corporate behavior in the past. If the investigation of the accident yields no identifiable villain, the media and the public are often skeptical and may claim wrong-doing is being covered up. Accident explanations invoking Knightian uncertainty are particularly suspect, because no blame can be assigned for failing to foresee an unforeseeable event.

What is relevant for our discussion of engineering failure is that the widespread desire to identify villains, when an accident occurs, has an effect on the media, juries, judges, and the general public. Leaders of engineering societies and state engineering-licensing boards live and work with non-engineer friends and neighbors, read the same newspapers, watch the same news broadcasts, and are affected by the general climate of opinion. The result is that despite attempts to exercise independent professional judgment, engineering leaders' opinions about what constitutes "the standard of care" and "ordinary prudence" can be influenced by public opinion and by the corresponding need to demonstrate concern for the public's well-being.

4.2 Punishment

If an engineer has been found to have acted negligently, punishment is usually administered through: 1) loss of license, 2) fines, 3) imprisonment, or 4) reputational damage. Reputational damage results from media coverage and from the actions of professional societies in issuing statements condemning the engineer's conduct and in expelling the engineer from the society. Having one's name associated with a widely publicized engineering failure may make future employment as an engineer difficult or impossible.

As has been mentioned previously, an ideal investigation would focus on what can be learned from an accident so that similar accidents can be prevented in the future. An unfortunate side effect of using the investigation results to identify wrong-doers and then punish them is that these actions make it more difficult to learn what caused the accident. People who fear being publically blamed and fear losing their license and livelihood as a result—or fear being criminally prosecuted—may not cooperate with investigators and may hire defense attorneys who advise them not to volunteer information.

5 Biases in failure investigations

Failure investigations are susceptible to two common biases that may arise when judging the actions of people well after an event has occurred and has been publicized. These biases are the "retrospective fallacy" and the "myth of perfect engineering practice."

5.1 Retrospective fallacy

The retrospective fallacy is frequently present in media reports of engineering disasters but at times is also present in the reports of technical specialists. The fallacy consists of making judgments about the past based on knowledge that became available only after the disaster occurred. As an example, consider what sometimes happens when technical specialists are called in to investigate the causes of an engineering disaster. After interviewing designers and reviewing documents related to the project, the investigators construct a story that explains how decision-makers failed to assess risks properly, failed to heed warning signs, failed to communicate, used out-of-date information, ignored quality-control, took large risks for personal gain, etc. All of which may be true, but the story is constructed by *selectively focusing on those events that are known to be particularly important only in retrospect*, that is, *after* the failure has occurred and observers look back at them. Before the failure, these events may not have stood out from dozens or even hundreds of other events (In the period before the disastrous failure of the Challenger Space Shuttle, NASA classified *745 components* of the Shuttle as "Criticality 1," meaning failure of the component would cause the loss of the crew, mission, and vehicle [9]). To the extent that investigators retrospectively identify events as particularly important—even though the events may not have been thought particularly important by competent people working at the time— then the investigators are committing what the sociologist, Diane Vaughan, has referred to as the "retrospective fallacy." [10, p. 68-70]

In determining whether engineers have been negligent, avoiding the retrospective fallacy is both important and difficult to do. *After* the disaster, it is often a straightforward matter to pick out specific decisions and claim that the decision-makers have been incompetent or negligent.

But in determining if engineers were or were not negligent, the key question is, "What did they know or could be reasonably expected to have known before the accident?"

The definition of negligence given previously refers to the standard of care that someone of ordinary prudence would have exercised under the same circumstances. "Same circumstances" means, among other things, avoiding the "retrospective fallacy."

5.2 The myth of perfect engineering practice

In addition to identifying the retrospective fallacy, Prof. Vaughn has identified what she has called "the myth of perfect engineering practice," which applies more to immature technologies than to mature technologies. As is the case of the retrospective fallacy, the myth may arise when looking back with a viewpoint biased by knowing what has happened. The mere act of investigating an accident can cause us to view, as ominous, facts and events that we otherwise would consider normal [10, p.200]:

> "When technical systems fail, … outside investigators consistently find an engineering world characterized by ambiguity, disagreement, deviation from design specifications and operating standards, and ad hoc rule making. This messy situation, when revealed to the public, automatically becomes an explanation for the failure, for after all, the engineers and managers did not follow the rules. … [On the other hand,] the engineering process behind a 'nonaccident' is never publicly examined. If nonaccidents were investigated, the public would discover that the messy interior of engineering practice, which after an accident investigation looks like 'an accident waiting to happen,' is nothing more or less than 'normal technology."

Thus in reading reports of an investigation into the causes of an engineering failure, just because some of the engineering practices described are not neat and tidy processes in which consensus is always achieved and decisions are always based on undisputed and unambiguous data, those facts alone may not explain the disaster; such practices may simply be part of normal technology—that usually results in a nonaccident.

6 Types of failure

Several case studies will be presented in the next section. In each study, the presence of one or more of the topics described above—negligence, standard of care, risk, uncertainty, bias, and punishment —discussed above will be pointed out. In addition, the type of failure will be proposed based on the following possibilities:

Negligence. Someone acted negligently (standard of care exercised by a prudent person).

Rare failure mode. A known and well understood failure mode of low probability occurred (acceptable risk).

Overlooked failure mode. A known and well understood failure mode was overlooked. Somebody blundered—they were not greedy or irresponsible; they worked hard and tried their best but, being human, they simply missed something.

Incorrect assessment of a known risk. A risk calculation for a known failure mode turned out to be incorrect. The technology was immature, and the project was complex.

New failure mode. A previously unrecognized failure mode occurred (Knightian uncertainty).

7 Case Studies

Case Study No. 1: The Great Boston Molasses Flood of 1919

Figure 1. Aftermath of molasses tank failure

Around mid-day on January 15, 1919, in Boston's North End, a large molasses storage tank—50-ft high and 90-ft in diameter—burst with a long rumbling sound and a noise like a machine gun as rivets popped out of the steel walls. Molasses released from the tank formed an 8 to 15-feet high wave traveling at 35 mph throughout the surrounding neighborhood, smashing railroad cars, lifting buildings off their foundations, and bending girders of a nearby elevated railroad. After the wave died out, a pool of molasses about 4 feet deep extended for 300 feet from the tank and then thinned out with further distance from the tank. People and horses caught by the wave fought to escape but only sank further into the sticky liquid. The final human toll was 21 people dead and 150 injured. About half of the deaths occurred the day of flood as a result of drowning or being crushed by the wave's impact; the other half of the deaths occurred in the following days as a result of injuries and infections. [11, 12, 13]

Clean-up consisted of hosing the area with salt water and then spreading sand on the streets. Water in the Boston harbor turned brown from the molasses washed from the streets. Rescue workers, cleaning crews, and spectators who flocked to the scene of the flood got molasses on

their shoes and clothing and thus managed to spread a sticky layer of goo to streetcar seats and public telephones throughout Greater Boston. "The smell of molasses remained for decades a distinctive, unmistakable atmosphere of Boston. " [14]

The molasses storage tank had been built in 1915 by the Purity Distilling Company, a subsidiary of U.S. Industrial Alcohol (USIA), to store molasses imported from the West Indies—the molasses was a by-product of refining sugarcane into sugar. Molasses was transferred, as needed, onto railcars to be carried to USIA's manufacturing plant in East Cambridge. The plant would distill a small amount of the molasses into grain alcohol for rum, but most of the molasses was distilled into industrial alcohol that could be sold to weapons manufacturers for the production of dynamite, smokeless powder, and other explosives. [12]

World War I was going on at the time that the tank was being built, and the market for munitions was strong. In a rush to finish the tank and take advantage of the increased demand for molasses, the company hurried construction, and the tank was not adequately inspected nor tested for leaks by filling it first with water—decisions made by the company treasurer, who was in charge of construction even though he had no engineering background. The completed tank showed clear signs of structural distress, as each time it was filled, it "groaned and shuddered," and neighborhood children were able to fill cans with molasses by holding them next to the numerous leaks. "In response to complaints, the company painted the steel-blue tank a brownish-red, presumably to camouflage the leaks." [11] When a laborer brought actual shards of steel from the tank's walls into the treasurer's office as evidence of the potential danger, he replied, "I don't know what you want me to do. The tank still stands." [12]

Law suits related to the tank failure lasted for six years, and over 3,000 witnesses gave testimony. Expert witnesses alone produced more than 20,000 pages of testimony, much of it conflicting. Three possible explanations for the failure were proposed: 1) Fermentation had produced high gas pressure within the tank; 2) anarchists had set off a bomb (such bombings had occurred at American industrial plants in recent years); and 3) the tank failed from structural defects. At the end of the trial, the court ruled that even though the cause of the failure could not be determined precisely, USIA was liable because the factor of safety in the original design was too low, and the company had ignored numerous signs that the tank was not sound. The

company paid between $500,000 and $1,000,000 total, with relatives of deceased victims getting about $7,000 each.

In 2014, Ronald Mayville, a senior structural engineer in the Massachusetts consulting firm of Simpson, Gumpertz & Heger, published an analysis of the causes of the failure. [15] He agreed with the court's observation that the tank walls were too thin—leading to the low factor of safety. But Mayville went further. He applied the design methodology given in a 1913 textbook to check the design of the riveted joints and found that the allowable stresses were exceeded. Next he used a finite-element analysis to show that stresses were very high at the rivet holes near the 20-inch manhole located at the base of the tank. His finding confirmed expert testimony at the trial that pointed to these rivet holes as the location where a crack originated and then spread rapidly across the tank.

Finally Mayville pointed out a contributing cause that could not have been known at the time of the failure, because the science of metallurgy was not sufficiently advanced: brittle fracture of the wall brought on by the low manganese content of the steel. Mayville cited data showing that the transition temperature—that is, the temperature at which ductile behavior transitioned to brittle behavior—of the steel "could have been as high as 59°F." The air temperature the day of the failure was about 40°F, and thus the steel was in a brittle condition. Two days before the failure, a tanker from Puerto Rico had arrived, and the tank was filled to *near capacity*. Even though the tank was filled thirty times over its lifetime, only five of the fillings (including the Puerto Rico tanker in the total) were to near capacity. Mayville suggested that "Perhaps the last few and greatest fillings of molasses were sufficient to then grow a crack to a critical size in a susceptible, brittle material, leading to the complete rupture of the tank, and the loss of 21 lives." [11]

Discussion of the Great Boston Molasses Flood of 1919

The failure of the structural designer to achieve an acceptable factor of safety in selecting the wall thickness is simple negligence. A similar conclusion applies to the failure of the designer to apply design methodology known at the time to check the design of the rivets. Yet another instance of negligence was the failure to investigate why the tank groaned when being filled and

why the tank leaked profusely—certainly not behavior within the range of "normal." Because these observations refer to a standard of care known at the time, they are free of the retrospective fallacy. A finite-element analysis was of course not available in 1915 but was not needed to design the tank.

The only aspect of the tank failure that makes it a case of something more than mere negligence is the role played by metallurgy. The ductile-brittle transition of the low-manganese steel used in the tank was not understood at the time. Thus to the extent that the low temperature on the January day of the failure caused brittle fracture to occur, tank failure by brittle fracture was a "new failure mode," and the design of the tank involved an immature technology. On the other hand, the negligence in design cited above may have been sufficient to cause the failure by itself. Not enough evidence is available to decide the question.

Case Study No. 2 Bangladesh Building Collapse

Figure 2. Aerial view of collapse.

On April 24, 2013, one of the deadliest structural failures in history occurred in an industrial suburb of Dhaka, Bangladesh. An eight-story reinforced concrete building housing shops, apartments, a bank, and—most significantly—five garment factories collapsed, killing 1,129

people and injuring approximately 2,000. Investigations after the collapse revealed many irregularities. [16, 17]

The building, called Rana Plaza, had been built in 2006 by Sohel Rana, who according to local officials and news media accounts [16], made money from illegal trading in drugs and guns, and traveled with his own motorcycle gang, which he used to intimidate people. He was nominally only a minor official in a local political organization but had strong influence among elected officials—"Money is his power," said a former mayor. To build Rana Plaza, Rana and his father acquired land from local landowners through intimidation and outright force. Because of his political connections, the police did not intervene. Even though his claims of title to the land were questionable, Rana was able to obtain an "informal" construction permit from the chairman of the local municipality, who was a political friend. [18] Rana thus avoided the need to get his building plans reviewed by the agency in charge of building safety. Later investigation found that the building had been constructed on the site of a former rubbish-filled pond and had been constructed of poor-quality materials. [17, 19, 20]

After the building had been used for several years, Rana saw an opportunity to take advantage of the rapid growth of Bangladesh's garment industry—Bangladesh had at the time more than 5,000 garment factories employing more than 3.2 million workers [17, 20]—and so added three floors to the building to rent to garment factories. Again he proceeded without obtaining a proper permit and review by the building safety agency. In time, five factories were established in the upper floors, and several thousand workers were employed there.

Because of the unreliability of electric power from the local electric utility, heavy diesel generators had been placed on the roof of the building. The vibration from the generators caused the building to shake when they were turned on. The architect who designed Rana Plaza in 2004 stated that he had been asked "to design a commercial shopping mall" that would contain shops and offices. He explicitly stated that Rana Plaza was designed for commercial use, not industrial use, especially industrial use involving the weight and vibration of heavy machinery. [21]

On the morning before the day of the collapse, garment factory workers on the third floor were frightened by a large noise and by big cracks suddenly appearing in a wall. A structural engineer named Abdur Razzak Khan was called in to investigate. Upon seeing the size and location of the cracks, Khan was horrified and told one of Rana's aides that the building should be evacuated immediately. [16, 18] In a television broadcast that evening Khan stated that the building was unsafe. [22] That afternoon, however, a local government official—who was *not* from the building-safety agency—visited the site and after meeting with Rana declared that the building was safe, pending another inspection. [18] Rana then spoke to the media, declared the building safe, and urged the factory workers to return to work the next day. The factory managers ordered their workers to return, threatening to cut their pay if they did not show up.
The next morning, according to witnesses, Rana told people gathered outside the building that it was safe. Slightly more than 3,100 people were in the building when the power from the electric grid went out. Generators were turned on, shaking the structure, which was already weakened from previous cracking. About 15 minutes later, the building collapsed.

In subsequent weeks, Rana was arrested as were three engineers, four factory owners, and various government officials responsible for approving building permits—all together, dozens of people were arrested. One of the engineers arrested was Abdur Razzak Khan— the same engineer who had inspected the building the day before the collapse and who had recommended that the building be evacuated. Khan was arrested, and charged with negligence, because he had helped the owner add the three floors to the building illegally. [19, 22]

Discussion of building collapse

This case differs from many cases of ethical failure in that negligence is so obvious. The owner, Rana, was not an engineer, but he employed engineers, who had a legal and ethical duty to ensure the safety of the public. The construction of an eight-story reinforced concrete building, preparation of an adequate foundation, and design for vibratory loads are all mature technologies, and thus the required standard of care was well-known but was ignored. Similarly the engineers were complicit in the owner's devious behavior in avoiding review of the plans by the government permitting agency, which if done diligently would have shown the inadequacy of the design and thus have prevented the collapse. The engineers failed to exercise the standard of

care expected from a prudent engineer under similar circumstances. Their behavior departed so far from that expected of a prudent engineer at the time that there is no question of committing the retrospective fallacy in making this judgment.

Case Study No. 3: Mrs. Hodges' House

Engineers were not involved in this incident, but it has been included in the case studies because it so clearly and dramatically indicates that "acceptable risk" does not mean absolute safety.

On the afternoon of November 30th, 1954, Ann Hodges of Sylacauga, Alabama, was at home napping peacefully on her couch when an object the size of a grapefruit crashed through the ceiling, bounced off a heavy radio cabinet, and struck her on the hip and the side of the torso, causing severe bruising. [23] Mrs. Hodges had thus become the first person in the history of the world to be confirmed as having been struck by a meteorite. (Readers might think about Mrs. Hodges the next time they curse their luck upon hearing that their flight is delayed three hours.) The meteorite later became known in scientific circles as "the Hodges meteorite," and a piece of it resides in the Smithsonian Institution to this day.

Discussion of Mrs. Hodges' House

It seems safe to assume that the builder of Mrs. Hodges' house did not take meteorite impact into consideration when constructing the house. It also seems reasonable that had he done so, he would have concluded that the probability of a meteorite striking the house and causing the roof and ceiling to fail was so small as to constitute an "acceptable risk," that is, the house was "safe," at least as far meteorite impacts were a concern. But "safe" does not mean failure was "impossible," and Mrs. Hodges had a nasty bruise to prove it. She simply had the misfortune to be involved in a painful way in a very improbable event. In terms of types of failure discussed previously, Mrs. Hodges' house experienced a "rare failure mode." The meteorite strike was not an example of Knightian uncertainty because from knowledge of the earth's size and of meteorite frequency, it was possible to estimate the probability of the strike, which would have been small. The builder was not negligent.

Case Study No. 4: Crash of Concorde

Figure 3. Concorde

On July 25, 2000, an improperly installed 1.1 m by 0.33 m titanium strip fell off a Continental Airlines DC-10 as it took off from Charles de Gaulle Airport near Paris. The strip lay unnoticed on the runway a few minutes later as a supersonic Concorde passenger airliner sped along the same runway prior to take-off. Because Concorde's wings were designed to develop lift efficiently at supersonic speeds rather than at lower speeds, take-off and landing speeds were much higher than those of subsonic airliners, and the Paris Concorde was traveling at a speed of about 210 miles per hour when one of its tires ran over the strip [24-FAQs]. The tire burst and pieces of tire were thrown violently against the underside of the wing. A fuel tank contained in the wing began to leak, and the leaking fuel then caught fire as the plane was leaving the ground. The airplane flew on for about a minute but lost engine thrust and crashed into a hotel, killing all 100 passengers, nine crew members, and four people in the hotel. [8, p. 175; 19, return to flight, Ch. 2]

After studying the causes of the crash, engineers modified the plane by installing a Kevlar lining in the fuel tanks. [8; 19-return to flight, Ch. 4]. A recently developed burst-resistant tire was also adopted. To lessen the possibility of electrical arcing igniting leaking fuel, additional shielding was installed to cover the electrical wiring in the undercarriage area. After many certification tests, Concorde service to New York was re-established on November 7, 2001. [24, history/00s] Concorde was discontinued in 2003 for financial reasons.

Concorde had been developed and manufactured jointly by the French company Aerospatiale and the British company British Aircraft Corporation as a supersonic airliner capable of cruising at a maximum speed near Mach 2—about 1350 miles per hour. Most Concorde flights were between London or Paris and New York or Washington. Because of its speed Concorde took about three and a half hours on these routes, while commercial subsonic flights took a little over twice as long. [25, p.225] Only twenty Concordes were ever built, and only fourteen were placed in airline service, beginning in 1976. The investigative report issued after the accident observed that "despite twenty-five years of commercial operations, the total number of cycles or flying hours performed by Concorde is clearly lower than that of other civil transport carrying out comparable stages." [8, p. 145] By the year 2000, the Concorde fleet had flown 235,000 flying hours, while a comparable passenger airliner fleet, the Airbus A300, had flown 5,645,000 hours. The report continued, "failures in many of Concorde systems and equipment, such as the tyres, engines, emergency slides or hydraulics, are relatively more frequent than on other aircraft currently in service. The complexity of Concorde as well as the era in which it was designed may explain this significant difference." Furthermore "the small number of Concordes in service impeded the treatment of problems encountered in operation, …" and "explains the slow rate of evolution of the aircraft." [8, p. 171]

Discussion of Concorde Crash

The investigative report's reference to Concorde's "slow rate of evolution" is another way of saying that Concorde was an immature technology. Also, the report stated that "[t]his accident was not predictable," [8, p. 171] thus indicating Knightian uncertainty rather than a miscalculation of risk. That the original designers failed to identify the failure mode—a burst tire leading to fuel-tank penetration and a fire—is shown by the manner in which the airplane was modified after the crash. All three modifications were aimed at decreasing the likelihood of a tire burst damaging the fuel tank and a fire breaking out. Thus it appears that the Concorde crash was an engineering failure but not the result of negligence.

Ten years after the accident, on December 6, 2010, a French court disagreed with this conclusion, as it convicted Continental Airlines and one of its mechanics of involuntary manslaughter. Two years later, a French "appellate court overturned the conviction, saying

mistakes by Continental mechanics were not enough to make it legally responsible for the deaths." [26] That the two courts came to opposite conclusions about the case indicates that they found the ethical issue a close call.

Several aviation lawyers were critical of the decision to prosecute Continental in the first place. "'Unfortunately we have zealous prosecutors and courts conducting these decades-long criminal investigation and prosecutions which serve no useful purpose,' said Kenneth Quinn, head of a safety task force for the International Civil Aviation Organization. Pursuing criminal charges "has been the single largest impediment to the objective investigation of these incidents that we've had," said Jeff Shane, an aviation lawyer at the law firm Hogan Lovells LLP. [26]

Case Study No. 5: Therac-25 Radiation Overdoses

Between June, 1985, and January, 1987, a total of six patients at cancer-treatment centers in the U.S. and Canada accidently received massive overdoses of radiation. All of the patients had been given radiation therapy from the same type of machine, a "Therac-25", and all suffered severe radiation burns. Three died. After the accidents, an investigation found errors in programming the Therac-25's computer that under certain conditions led to radiation levels much higher than the intended dosages. [27, 28, 29, 30]

The Therac-25 was a "medical linear accelerator," designed and sold by a company called Atomic Energy of Canada Limited (AECL), and used to produce radiation to destroy malignant growths without damaging surrounding healthy tissue. Eleven Therac-25s were operating during the 1985-87 period. The machines were controlled by PDP-11 computers programmed in assembly language.

The Therac-25 was intended to replace two earlier accelerators, the Therac-6 and Therac-20. All three accelerators had the potential of producing beams of radiation so concentrated and powerful that patients would suffer severe radiation burns if accidentally exposed to the unmodified beams. The Therac-20 prevented such accidents from occurring by relying on mechanical safety features such as hardware interlocks. In contrast, the Therac-25 relied on software to ensure that the machine was operated in a safe manner. This design decision turned out to be pivotal, as software errors similar to those found in the Therac-25 were later found to

be present in the Therac-20 too, yet no injuries resulted from the Therac-20—its hardware interlocks had prevented radiation overdoses from occurring.

The first radiation overdose occurred at a clinic in Marietta, Georgia on June 3, 1985. The patient later stated that she had felt a "tremendous force of heat … this red-hot sensation," and she told the technician, "You burned me." [28] The hospital physicist called AECL to ask if such a burn was possible in the therapy mode in use at the time, and three days later was told in a phone call that the burn described was not possible. The patient filed a lawsuit on November 13, 1985, and thus AECL executives must have known about the incidence by that date, but the company did not initiate an investigation.

The second overdose occurred at a Hamilton, Ontario, clinic on July 26, 1985. When the operator turned on the machine, it shut down after five seconds and displayed an error message "H-tilt." The documentation supplied by AECL did not explain what the various error messages meant. The machine also displayed a message "no dose" that indicated no radiation had been delivered to the patient. The operator attempted four more times to get the machine to function but to no avail. A technician was called in but could find no problem. Even though the "no dose" message had been displayed after each attempted treatment, the patient soon developed signs of severe radiation burns. AECL, the U.S. Food and Drug Administration and its Canadian counterpart were informed. AECL attempted to reproduce the malfunction on its own machine but failed. Nonetheless AECL suspected a problem with some microswitches and so modified them. It then reported to the hospitals that "analysis of the hazard rate of the new solution indicates an improvement over the old system by at least five orders of magnitude."

The third overdose occurred at a Yakima, Washington, hospital in December, 1985. An unusual striped pattern had developed in the patient's skin after one of the treatments. Hospital personnel informed AECL of this symptom on January 31 and several weeks later received a response from the AECL technical support supervisor saying, "After careful consideration, we are of the opinion that this damage could not have been produced by any malfunction of the Therac-25 or by any operator error." [28]

The fourth overdose occurred on March 21, 1986, and the fifth on April 11, 1986, both at a cancer-treatment center in Tyler, Texas. After the March incident, two AECL engineers came to

investigate but could not reproduce the "Malfunction 54" error message that the machine operator had observed. One of the engineers explained to the hospital physicist that it was impossible for a patient to receive an overdose from the machine. The physicist claimed later that he had asked AECL if any other overdose injuries had been reported by other users of the Therac-25, and he was told that there were none—even though the Hamilton and Yakima incidents had already occurred. AECL engineers suggested that the Tyler patient's burns were caused by a faulty electrical power circuit. The hospital hired an engineering consulting firm to check the circuit, and the firm reported that it could find nothing wrong.

After the second Tyler incident, on April 11, the hospital physicist prohibited further use of the machine and began a painstaking investigation. Working closely with the machine operator, who remembered exactly what steps she had followed in entering instructions via the keyboard, the physicist was, after many hours of effort, able to consistently reproduce the Malfunction 54 error message. He was able to show that the error arose—and an overdose delivered—when the operator 1) made a certain mistake in entering data, and 2) typed very fast when correcting the mistake. The Therac-25 software contained an error that produced an improper (and dangerous) machine setting when conditions 1) and 2) existed. AECL was informed of the error but could not reproduce the error on its own machine until the physicist explained that typing speed played an essential role. Possibly a reason that the error had not been detected during software-development tests at AECL was that the operator-tester never developed the typing speed that an operator at a hospital would develop after using the machine repeatedly over a year or two.

The sixth overdose occurred at the Yakima, Washington, hospital on January 17, 1987. This time AECL engineers found a software error *different* from that found in the Tyler incidents. It was not possible to determine if either the Tyler software error or the 1987 Yakima software error also caused the Hamilton, 1985 Yakima, or Marietta overdoses. Given that two errors had already been discovered in the software, it may have been possible that yet undiscovered errors were responsible.

Leveson and Turner [28] summarize the factors that contributed to the Therac-25 incidents:

- management inadequacies and lack of procedures for following through on all reported incidents,

- overconfidence in the software and removal of hardware interlocks (making the software into a single point of failure that could lead to an accident),
- presumably less-than-acceptable software-engineering practices, and
- unrealistic risk assessments along with overconfidence in the results of these assessments.

In February, 1987, the FDA declared the Therac-25 to be defective and should not be used again until the deficiencies were remedied. In July of that year, the FDA approved AECL's Corrective Action Plan.

Discussion of Therac-25 Radiation Overdoses

The type of failure appears to be that of an incorrect assessment of a known risk—the possibility of radiation burns from incorrect use of a medical linear accelerator. The Therac-25 was an example of immature technology: a retrospective perspective shows that 1) software design and testing were inadequate—in fact, the Therac-25 story is now considered a standard software-engineering case-study that shows the need for adequate testing; 2) AECL apparently lacked an established, aggressive procedure to respond to and investigate reports of accidents;
3) redundancy in interlocks (both software and hardware) was needed; and 4) Thera-25 engineers grossly under-estimated the probability of radiation burns. In light of the principles of the retrospective fallacy and the myth of perfect engineering practice, negligence does not appear to be an explanation for the accidents.

References

1. "Negligence." Legal Information Institute. Accessed February 9, 2015. http://www.law.cornell.edu/wex/negligence.

2. "PROFESSIONS, OCCUPATIONS, AND BUSINESS OPERATIONS (225 ILCS 325/) Professional Engineering Practice Act of 1989." Illinois Compiled Statutes.

3. "Report on the Practice of Forensic Engineering for the Colorado State Board of Licensure for Professional Engineers and Professional Engineers and Professional Land Surveyors." The Forensic Engineering Task Force. April 3, 2006.

4. "ASCE Code of Ethics, Canon 1." American Society of Civil Engineers. 2006.

5. Lowrance, William W. *Of Acceptable Risk*. Los Altos. William Kaufmann, Inc. 1976.

6. Knight, Frank H. *Risk, Uncertainty, and Profit*. Boston, MA: Hart, Schaffner & Marx, Houghton Mifflin Co., 1921.

7."Act of God." Legal Information Institute. Accessed February 9, 2015. http://www.law.cornell.edu/wex/act_of_god.

8. "Accident on 25 July 2000 at La Patte D'Oie in Gonesse (95) to the Concorde Registered F-BTSC Operated by Air France. Report translation f-sc000725a." July 25, 2000.

9. "NASA's Response to the Committee's Investigation of the 'Challenger' Accident." Hearing conducted by the House of Representatives Committee on Science, Space, and Technology. February 26, 1987.

10. Vaughan, Diane. *The Challenger Launch Decision.* Chicago, IL: University of Chicago Press. 1996.

11. Schworm, Peter. "Nearly a century later, structural flaw in molasses tank revealed." Boston Globe. January 14, 2015.

12. Puleo, Stephen, *Dark Tide*, Boston, Beacon Press, 2003.

13. Jabr, Ferris, "The Science of the Great Molasses Flood," Scientific American, July 17, 2013.

14. Park, Edwards, "Without Warning, Molasses in January Surged Over Boston," Simthsonian 14 No. 8, November 1983, pages 213-230.

15. Mayville, Ronald. "The Great Boston Molasses Tank Failure of 1919." CENEWS civil + structural ENGINEER, September 1, 2014.

16. Yardley, Jim. "The Most Hated Bangladeshi Toppled From a Shady Empire." The New York Times. April 30, 2013.

17. Yardley, Jim. “Report on Deadly Factory Collapse in Bangladesh Finds Widespread Blame.” New York Times. May 22, 2013.

18. Al-Mahmood, Syed Zain. "Nexus of Politics, Corruption Doomed Rana Plaza." Dhaka Tribune. April 26, 2013.

19. Hossain, Farid, and Julhas Alam. "Bangladesh Official: Disaster Not 'really Serious'" USA Today. May 3, 2013.

20. Ali Manuk, Julfikar and Yardley, Jim. **“**Building Collapse in Bangladesh Leaves Scores Dead.” New York Times**.** April 24, 2013.

21. Bergman, David. "Bangladesh: Rana Plaza Architect Says Building Was Never Meant for Factories." DailyTelegraph. May 13, 2013.

22. "Bangladeshi Engineer Arrested in Building Collapse." USA Today. May 3, 2013.

23. Nobel, Justin. "The True Story of History's Only Known Meteorite Victim." *National Geographic*, February 2, 2013.

24. "CONCORDE SST - The Definitive Concorde Aircraft Site on the Internet." CONCORDE SST - The Definitive Concorde Aircraft Site on the Internet. Accessed February 21, 2015. http://www.concordesst.com/.

25. Orlebar, Christopher. *The Concorde Story*. Seventh ed. Oxford: Osprey Publishing, 2011.

26. Jansen, Bart. "French Court Overturns Concorde Crash Conviction." USA Today. November 29, 2012.

27. "Fatal Radiation Dose in Therapy Attributed to Computer Mistake." The New York Times. June 21, 1986

28. Leveson, Nancy, and Turner, Clark S. "An Investigation of the Therac-25 Accidents" IEEE Computer, 26, No. 7, July 1993, pp. 18-41.

29. Casey, Steven. *Set Phasers On Stun.* Santa Barbara, Aegean, 1998.

30. Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley, 1995.

Photo Credits

Figure 1. By BPL via Wikimedia Commons

Figure 2. By Rijans007 via Wikimedia Commons

Figure 3. By Henry Salome via Wikimedia Commons