AC 2008-2051: UNDERSTANDING TECHNOLOGICAL FAILURE: ETHICS, EVIL, AND FINITUDE IN ENGINEERING DISASTERS

Gayle Ermer, Calvin College

Understanding Technological Failure: Ethics, Evil, and Finitude in Engineering Disasters

Abstract

It is important to know why technological systems sometimes fail catastrophically. Not only does culpability need to be established justly after a disaster, but the success of new technology depends on accurately predicting how technology and the individuals and societies with which it interacts will behave. It is nearly always the case that disasters occur due to the contribution of multiple factors. Sorting these factors into categories can help to better understand the nature of the factors and to ensure that all of the necessary categories are considered carefully in the design process. This categorization can also help engineering educators to make certain that all of the different categories are studied in the engineering curriculum in appropriate places. In this paper, the categories of individual ethical responsibility, societal evil, and human finitude will be used to discuss the character and importance of various contributions to specific engineering disasters. The technological systems to which these categories will be applied include the Helios Flight 522 crash, the Bhopal chemical plant gas release, and the Three Mile Island nuclear reactor near melt-down.

Causes related to personal ethics include the immoral actions of people that contribute to catastrophic failures. This type of cause is usually opposed in the engineering curriculum through the study of engineering codes of ethics and case studies to help students clarify the moral responsibilities inherent in their chosen career and to apply them faithfully. Causes related to societal evil include the political and economic contexts in which modern technology operates that contribute to engineering disasters. While some of these issues are dealt with in the context of engineering ethics, often they are better dealt with in liberal arts courses which intentionally raise the consciousness of students to their importance. Societal issues should also be brought into engineering technical courses as frames for design work. Causes related to human finitude include the limitations of our predictive models and the characteristics of modern technology that make catastrophic failures more likely. Engineering disasters cannot be avoided solely by training engineers to be more ethically responsible. Engineering instructors and students need to be aware that the nature of the technological systems in North American society and the means by which these systems are designed and controlled all contribute to the catastrophic potential for technological failures.

1. Introduction

On August 1, 2007, evening rush hour traffic in Minneapolis was bumper-to-bumper on the I-35W bridge over the Mississippi River. Shortly after 6:00 pm, a 500 foot long span suddenly collapsed, sending cars and debris into the river over 100 feet below. Thirteen people were killed

in the collapse and almost 100 were injured.[1] What caused this tragedy? Was it a technical design flaw? Are other bridges at risk?

Like many engineers, I am concerned about and intrigued by situations in which technological designs do not behave as predicted. When human death and injury occur because of a failure of engineering, I want to know why that failure occurred, not just to satisfy my own curiosity but to learn from the errors of history. It is important for all people involved with modern technology to know why catastrophic failures occur. Not only does blame need to be assigned justly in these situations, but the avoidance of such failures in the future depends on accurately predicting how technology and the individuals and societies with which it interacts will behave.

To avoid future disasters, it is important that we have an accurate and complete understanding of the nature of the different causes that contribute to them. This paper will use the categories of failure of personal ethics, societal evil, and human finitude to characterize the nature of different contributions to technological disasters. These categories arise from a robust understanding of what it means to be part of a natural world that we do not completely understand and a cultural world that is often not considered carefully enough when new technology is introduced. It is hoped that this clarification of categories will provide a better understanding of the ways in which technological systems can go wrong. The use of these categories can alert engineering educators and others to aspects of technology that are often underemphasized and should be articulated more clearly to the students we teach, who will become the directors and caretakers of technological systems for the future. This categorization recognizes that engineering disasters, like most other events, are typically more complicated than they seem, and will ensure that adequate attention is given to different aspects of engineering activity that can contribute to safer designs.

Before the categories are described, it is necessary to provide some background on technology in general and how engineers relate to modern technology. Section 2 will present this background. Section 3 will describe the categories in detail, including how these categories relate to the characteristics of modern technological systems. Section 4 will analyze several engineering disasters in order to see how and to what extent factors from the different categories contributed to the failures and how they can be used to help classify potential future risks. These can also serve as case studies for discussion of technological risk in engineering courses or in liberal arts courses that reflect on the role of technology in society. The paper will conclude with some recommendations for what we need to do as engineers to reduce the risk of engineering disasters and how we can integrate the awareness of these concepts into the experiences of undergraduate engineering students.

2. Technology, Engineering and Risk

Doing technology is central to what we are as humans. Anthropologists have chosen to describe the first modern humans as “homo habilis,” therefore expressing the centrality of our “tool-using” and tool creating capabilities to our very nature.[2] But, everyday observation reminds us that technology, like all other human cultural activities, is not perfect. Technological failure can have catastrophic consequences. Technology can be done negligently. Technology can be intentionally misused. The current technological systems of the developed world continue to engender negative as well as positive consequences to our natural and social environments.

As a foundation for understanding technological failure, we need to clarify what is meant by the terms “technology” and “engineering”. Many philosophers of technology emphasize that technology is a human cultural activity. This is a different perspective from that of the general public or even of many practicing engineers, who limit their concept of technology to particular contemporary objects or physical systems. Carl Mitcham, in his book *Thinking Through*

Technology, observes that one commonality among the definitions of technology prevalent among those who consider technology from a philosophical perspective is that in every case "technology is pivotally engaged with the human." He goes on to assert that "as such it is to be considered in relation to the essential aspects of a philosophical anthropology – with differences drawn between its manifestations in the mind, through bodily activities, and as independent objects that take their place in the physical and social world."[3] Mitcham distinguishes between four modes in which technology is actualized: technology as volition, technology as knowledge, technology as activity, and technology as object. It seems clear that the first two manifestations of technology described are necessarily involved with the morals and ethics of individual humans. It is human agents who make design decisions and hold the knowledge of technological processes. It also seems clear that these human agents do not operate by themselves, but participate in society and are influenced by others around them. Therefore societal and cultural practices have an influence on technology and are in turn influenced by new technology. The second two modes emphasize that the physical world is clearly involved in the engineering design process. The objects designed and the tools used to form those objects all utilize materials whose behavior is not completely understood and involve systems with very complicated interactions between the objects and the humans who use with them. This definition also implies that the four modes of technology manifestation may look very different at different times in history. This opens the door to the possibility that there may be characteristics inherent in current technological systems that push the limits of acceptable risk.

Engineers are important actors in technology. In our contemporary situation, it is engineering design, "the systematic, intelligent generation and evaluation of specifications for artifacts whose form and function achieve stated objectives and satisfy specified constraints" that contributes substantially to the form and function of the technological products that are ubiquitous in our modern world. [4] Our actions as engineers are often more constrained by economic and political considerations than we would like to admit, but engineers do stimulate the development of new technologies and control many aspects of technology implementation. It is in the engineering design process that decisions are made by engineers which will significantly effect how technological systems end up being constructed, maintained, and utilized including the potential risk for catastrophic failure.

3. A Robust Understanding of Contributions to Failures

The categories that I have chosen to characterize the nature of different contributions to technological disasters include the concepts of 1) individual immorality, which focuses on the unethical choices and immoral dispositions of people that contribute to engineering disasters, 2) societal evil, which focuses on the pervasive bad influences of the cultural and social institutions within which our designs are embedded, and 3) human finitude, which relates to the capabilities of humans to adequately predict how technological objects will behave in real life situations and to cope with those limitations. An appreciation of each of these explanations for why technological systems fail can contribute to more perceptive judgment of the risks of various designs.

3.1 Personal Ethics

Causes related to personal ethics include the immoral actions of people that contribute to catastrophic failures. People are not always careful or diligent or loving of their fellow humans when they do technology. People design, manufacture and use technology to deliberately hurt other people. People have always tried to hurt other people, but technology certainly increases their power to harm. This type of cause is usually addressed in the engineering curriculum through the study of engineering codes of ethics and case studies to help students clarify the moral responsibilities inherent in their chosen career and to apply them faithfully. Efforts to

infuse ethical considerations throughout the technical part of engineering curriculum can be particularly effective in preparing students to be aware of potential ethical violations and provide them with the knowledge and judgment needed to make ethical choices. One limitation of this approach is that it assumes that all people are well-intentioned and governed by logic in deciding how to behave. Often, discussions of the ideals of the engineering profession can help to convince students of the benefits that the engineering profession provides for individuals and society and the need for them to be committed to those ideals. But, in many cases of technological malfeasance, the individuals involved were concerned only with their own interests at the expense of the interests of the profession or allowed impulsive desires for convenience, profit, power, or recognition to influence their decisions. The fact is that while many engineers recognize what the standards of ethical conduct require, some still participate in actions which fall short of that standard. The engineering profession needs to recognize the effects that deliberate choices can have on the risk of technological failures by supporting regulatory systems that provide checks and balances so that unethical behavior can be detected before it has catastrophic effect. Holding responsible those who cause harm with technology through the legal system can also serve as a deterrent.

3.2 Societal Evil

Causes related to societal evil include the political and economic contexts in which modern technology operates that contribute to engineering disasters. For example, in a capitalistic economic system, the tendency to increase profits by cutting corners to reduce costs is a constant presence. In a socialistic economy, the lack of direct rewards for additional work can contribute to negligence. Whether in a democratic or totalitarian political system, there is a strong incentive for those in control to place the risks of technology disproportionately on those who have little representation. While some of these issues are dealt with in the context of engineering ethics, often they are better dealt with in liberal arts courses which intentionally raise the consciousness of students to their importance. For example, economics courses explore the nature of capitalism and its effects on individuals and institutions. This can be an opportunity for engineering students to reflect on how technology has been influenced by economic systems. History courses discuss the relationships between cultural context and technological developments in different societies. Since students do not always perceive their liberal arts courses as being relevant to engineering work, and since not all liberal arts instructors spend enough time relating their discipline to technological issues, it is also important that cultural context be brought into engineering technical courses as frames for design work.

Although societal evil results from the sum total of the ethical choices of many individuals, this category of causes needs to be handled differently from the category of personal ethics. Social and cultural practices are systemic, and often immune to control by particular individuals, except perhaps for a few with exceptional power and influence. There are two modes for addressing the corruption in our culture that affects engineering designs. The first mode involves working through the political process and other institutional pathways to curb the tendencies in culture which increase risk. The other involves increasing awareness of these issues during the design process so that checks and balances can be applied to make the design more robust to societal pressures.

We live in a culture that has been described as given over to "technicism"[5] or "technopoly."[6] These terms express the realization that contemporary North American culture overly relies on technical solutions to problems and has too much faith in science and engineering to give us power over the natural world and other humans. The tendency to idolize technology will increase the risks of technology. Without a respect for the limits of technology, technological development can take place at a pace that leaves no time for careful risk assessment. When all of reality is viewed from a technical, utilitarian perspective, the value of human life is often diminished

3.3 Human finitude

The category of human finitude can easily be overlooked as a primary contributor to the risk of failure in today's technological systems. Some of the disasters discussed later will be used to show that this category is growing in its contribution to the risks we live with on a daily basis. While it can often easily be seen how poor ethical choices or the temptation of cutting corners for economic reasons contribute to engineering failures, the fact that we are limited by our own capabilities is not often acknowledged, especially under the influence of modernist thinking which assumes that human nature and society can be never-endingly improved by applying our scientific knowledge.

3.3.1 Gaps in the Models

Humans are finite beings. Our observations of the world around us reveal an inexhaustible complexity of relationships and causes. Because of this, our physical models will never completely capture the actual way things behave. Our knowledge and our power will never be complete. Science has contributed many insights that are crucial to doing successful engineering work, and it continues to improve our predictive capabilities, but we will never arrive at a point where we have comprehensive knowledge of everything.

Henry Petroski supports this conclusion by stating that an engineered artifact is always a hypothesis which can be disproved by failure.

> "The process of engineering design may be considered a succession of hypotheses that such and such an arrangement of parts will perform a desired function *without fail*. As each hypothetical arrangement of parts is sketched either literally of figuratively on the calculation pad or computer screen, the candidate structure must be checked by analysis. The analysis consists of a series of questions about the behavior of the parts under the imagined conditions of use after construction…Absolute certainty about the fail-proofness of a design can never be attained, for we can never be certain that we have been exhaustive in asking questions about its future."[7]

Fortunately, engineering science gives us a great deal of understanding of the way things work, and we should be grateful that the vast majority of our modern engineering hypotheses turn out to be true, but our limited creativity has contributed to disasters as well. Martin and Schinzinger, in their widely used engineering ethics textbook, have a chapter on "Engineering as Social Experimentation" that also emphasizes the point that engineering projects are generally "carried out in partial ignorance."[8] The nature of engineering is to push the envelope. We are always operating at the edge of our ability to predict. This is intrinsic to the discipline (and part of what makes engineering fun), but it is also what makes engineering potentially dangerous.

The difficulty in predicting how technology will work also occurs beyond the physical/scientific realm. Technology is holistic: it touches all aspects of life as we live it. Lambert VanPoolen describes engineering as "prophetic activity."[9] Design is based on predictions about how an artifact will work in real life. Through engineering, a problem solution is taken from an abstract idea to a concrete implementation. At each step in that progression, we find that our predictions fall short. This explains, at least partially, why technology is risky. Since technology is often reduced to only its physical and logical aspects, it should be no surprise to find that our models do not adequately deal with the psychological and social effects of engineering designs.

The ability of human beings to make their own choices complicates our predictions about how they will interact with technological artifacts and opens up possibilities for unanticipated modes of failure. Users of technology often apply technological objects in ways the designers never intended. At the societal level, communities may react to new technologies in ways that were not

anticipated. In fact, all technology appears to generate unintended consequences that may be disastrous.[10]

3.3.2 The Nature of Modern Technology

One of the defining features of technology in the developed world today is its complexity. Disasters are often caused by interactions of several minor failures that were not anticipated because modern designs are so complicated. Charles Perrow suggests that the features of modern technology (complexity and tight coupling) make it almost inevitable that disasters will happen. He identifies these types of failures as normal accidents, implying that some technological systems are at particularly high risk of catastrophic failure. This can be interpreted as another manifestation of human finitude. Our technology may have outstripped our own ability as designers and operators to understand it.

Certainly many users of modern technological systems have very little understanding of or appreciation for what goes on behind the surface of technological artifacts. Albert Borgmann concludes that the current technological paradigm involves intentionally isolating the means of obtaining goods in order to eliminate the burdens associated with obtaining those goods. This involves the separation of the "machinery" of the technology from the ends it has been designed to achieve. He calls this tendency the "device paradigm."[11] This lack of technological transparency contributes to the possibilities that responses to small failures may accidentally result in disaster. If this is a true description of our modern engineering paradigm, then individual efforts to increase the safety of particular designs may be limited by the expectations and capabilities of technology users.

All modern technology has some level of risk. Every engineering code of ethics states that in engineering we must "Hold paramount the safety of…"[12] But, in reality all engineering design is based on compromise between multiple factors. Limited time and resources mean we must balance safety considerations with other goods. So, if safety cannot be held paramount (for example, a safer automobile would be too expensive) we need to decide as a community, with just representation of all parties affected by the technology, what is acceptable risk. The processes currently used to make these decisions are often hidden.

In summary, the category of finitude points us to a number of characteristics of human nature and modern technology which can contribute to failure despite the best ethical intentions of the people involved and apart from the motivations induced by corrupt social systems. It may also direct us to address system level constraints on engineering design activity in order to reduce risk of disaster.

4 Engineering Disasters Explained

The descriptive categories described above are useful in directing our attention to reasons for technological risk that are not often given enough consideration in the engineering analysis of disasters. Several examples of failure events will be analyzed to show how these categories can be applied to arrive at the best explanation for why a disaster occurred, leading to ideas for how disasters like these can be avoided in the future.

4.1 Helios Airlines Flight 522

On August 14, 2005 Helios Airlines Flight 522 departed from the Larnaca airport in Cyprus on its way to Athens. Ground control cleared the plan for a cruising altitude of 35,000 feet. A few minutes later, the pilots contacted the company Operations Center to report an air conditioning problem and a take-off configuration warning alarm. After communicating with a Ground Engineer for approximately 6 minutes, contact with the aircraft was lost. The plane continued to fly on its programmed path to the Athens airport and entered into a holding pattern. Two Greek

air force F16 fighter jets tried to intercept the flight, but as they flew alongside, the apparently helpless aircraft crashed into a wooded hillside. All the passengers and crew perished in the crash, a total of 121 people.

As in many technological failures, all of the causes of this incident were not immediately apparent and some remain controversial. The official Aircraft Accident Report[13] identifies both direct causes and latent causes. Among the direct causes are the non-recognition that the cabin pressurization mode selector was in the manual position (rather than automatic) during the preflight check and the non-identification of the reasons for the activation of various warnings during the flight. Incapacitation of the flight crew due to hypoxia was also indicated as a direct cause. The report notes that the pressurization mode switch was apparently not returned to the "AUTO" position after some earlier non-scheduled maintenance on the jet, but concludes only that this "could" have contributed to the accident. Analysis of the Flight Data Recorder after the crash contributed information to support the following interpretation of events. Because the pressurization switch was inadvertently set to manual as the flight took off, cabin pressurization did not take place as the flight gained altitude. As an altitude of 10,000 feet was passed, an alarm horn sounded, indicating the lack of oxygen being supplied to the cabin. Since this alarm also sounds to indicate problems with pre-flight conditions in the plane, the flight crew assumed the alarm was a mistake and contacted the Operations Center to determine what was wrong. As the jet continued to gain altitude, the passenger air masks were deployed, but by then hypoxia had impaired the ability of the crew to respond properly. Eventually, all aboard the aircraft became unconscious (except for a single flight attendant whom the F-16 pilot reported seeing moving about the cockpit), and the plane continued to fly on auto-pilot until it ran out of fuel and crashed.

Private investigations by the Discovery Channel appear to have uncovered another possible cause for the crash. They report on a design flaw in the wiring for the outflow valve for the pressurization system. If this flaw was present, the cabin pressure would have gone down due to an open outflow valve and the pressurization switch might have been set to manual by the pilots as an attempt to correct the problem. Previous maintenance records for the Boeing 737 also show a recent inspection of one of the cabin doors for possible leakage, although the door passed the inspection.

In either case, the path from a minor mistake during the pre-flight check or a technical design flaw or a component failure to a full-fledged disaster was compounded by the complexity of the systems involved (finitude) and possibly also by an atmosphere at this particular airline of lax maintenance and training of personnel (societal evil). Operator deficiencies were identified as a latent cause by the Incident Report and also inadequate execution of the regulatory authority's safety oversight.

It is worth noting that air travel, especially in the United States, is considered to be very safe. The total number of fatalities per year due to aircraft accidents is substantially (several orders of magnitude) smaller than the number of automobile deaths.[14] But, many fewer people fly than drive, contributing to a risk level per mile for driving that is in the same range as for flying. In other words, contrary to the popular wisdom used to reassure fearful airplane passengers, it is not safer to fly than to drive on a per mile traveled basis. From reviewing airplane crash explanations, it appears that finiteness considerations are responsible for many of the disasters. Often, even when the cause of a crash is attributable to operator error, the operator's choices were significantly influenced by the extreme complexity of the airplane and air control system and his or her inability to respond fast enough to changing conditions in situations of incomplete knowledge.

Purely "technical" failures also result in disaster much more often in the air travel system than in automotive travel. Airplanes function in a very demanding physical environment. The design of

an aircraft must include lower safety factors because an over-designed aircraft will use too much fuel or in the extreme case may not even fly. So, it is not unreasonable to think that the gaps in the modeling of material behavior within the aircraft structure and how those materials interact with the highly variable flight conditions might be responsible for not anticipating conditions that might cause failure.

4.2 Bhopal – A Disaster Waiting to Happen

In December of 1984, a Union Carbide plant producing pesticides in Bhopal, India suffered an accident that released deadly methyl isocyanate (MIC) gas into the atmosphere. Between 4000 and 7000 people were killed as a result of the accident. This event qualifies not just as a disaster, but as a catastrophe. It is one of the few accidents where "it could not have been worse." It takes just the right combination of circumstances to produce a catastrophe of this magnitude. The frightening fact is that it is quite likely that there are hundreds of chemical plants around the world in the same situation as Bhopal, which can be thought of as disasters waiting to happen.

The explanations for the incident included component failure combined with lax plant operation. Just a few months before the accident, inspectors found leaky valves, inaccurate instrumentation, poor training, insufficient staff, and inadequate safety devices at the plant. Although no particular individual deliberately compromised the safety of the surrounding community, it appears that many individuals made cost-saving choices in pursuit of profit that incrementally reduced the effectiveness of individual redundant safety systems in a way that left the plant as a whole particularly vulnerable to a serious accident. The local environment of the plant, consisting of a shanty town immediately outside the plant gates, was part of what turned the accident into a catastrophe.

The factory at Bhopal manufactured Sevin™, a pesticide which was designed to replace DDT (which was phased out due to its negative environmental effects). In 1980 the company added a unit to produce MIC and store it in two large tanks as a liquid under nitrogen gas pressure. Before the MIC production process was added, the chemicals used at the plant were not particularly dangerous, so housing was built nearly up to the gates of the facility. The plant was designed with several safety systems to prevent the release of toxic gas into the air. MIC from the storage tanks could be directed to a scrubber tower, where it could be chemically destroyed. A refrigeration system was implemented around the tanks to make sure the gas did not build up enough heat and pressure to force poison to gush through a safety valve. A burn-off torch was included, and a water spray was available, mostly to fight fires, but also to neutralize the gas. Before the accident (June), it was discovered that the refrigeration system was not working because the refrigerant had been siphoned off for use elsewhere in the plant. The scrubber tower had been turned off in October because MIC was no longer being produced, only stored at the site. At the time of the accident, the gas flare was shut down waiting for a part to repair a corroded pipe. Prior to the incident, there had been some trouble with the nitrogen gas pressurizing system – some water seeped into the pipes and chemically combined with the MIC to form sludge.

The accident was initialized when workers attempted to remove the sludge by running water into the pipes to flush it out through a drain. Before doing this they were supposed to place metal barriers in the pipes as a safety precaution to block water from getting into the tanks. The barriers were not installed because someone forgot (finitude). The drain was clogged causing the water to back up. Soon it rose to a level high enough to flow into the MIC tank through a valve in the piping system that should have been closed (and blocked by the forgotten metal barriers). More than 100 gallons of water gushed into the tank, starting a chemical reaction producing heat. The pressure in the tank went up, but operators did not react until it was off the instrument scale in the control room. The operators tried to respond, but there was nothing they could do to prevent the gas from venting: there was no refrigeration, they could not get the scrubber back on line, the

flare was disabled, and the water spray did not reach high enough to interact with the venting gas. As a result, MIC vented for two hours, hugging the ground.

Will we have more of these disasters in the future? The probability is not as low as we would hope. People familiar with the incident commented that there are many plants, in the US and around the world, which are operating under the same conditions as Bhopal before the accident. To avoid future incidents, engineers need to be encouraged to have the integrity to speak up when they see potentially unsafe conditions (personal ethics). Engineers need to promote the allocation of resources for regulation of chemical plants by industry self-policing and/or government inspection in order to reduce the incentive to cut corners to increase profits (social evil). They also need to have a constant awareness of the safety needs of the system as a whole, as well as focusing on particular safety devices (finiteness).

Three Mile Island – Normal Accidents

An accident typically happens due to the interaction of multiple failures. In the near disaster of the nuclear reactor at Three Mile Island, the complexity of the system caused trivial failures to combine in a way that was not foreseen. Charles Perrow points out that the potential for disaster tends to be higher in systems that are tightly coupled, meaning that elements of the system are very dependent on other elements with little time to intervene (chain reaction). Nuclear reactors are by their very nature tightly coupled. Another contributing factor was the fact that the reactor itself was contained inside a building such that the condition of the system could be monitored only through transducers and instrumentation.

Figure 3 shows the basic components of a nuclear reactor. On Wednesday, March 28, 1979 the Unit 2 Reactor near Harrisburg, PA was running smoothly. Starting at about 4:00 am, a series of inter-related failures occurred that nearly resulted in a core meltdown. The first failure consisted of a condensate leak from the condensate polisher. In response to this failure, the pumps in the secondary loop shut down. This was not an uncommon occurrence for the plant and systems were in place to respond to this failure. Since the turbine and pumping system were not operating, heat was not transferred out of the primary loop, causing the temperature and pressure in the primary loop to increase (as expected). The pilot operated relief valve (PORV) automatically opened, releasing steam into a holding tank. The secondary loop had backup pumps which should have automatically engaged when the main pumps turned off. Unfortunately, unknown to the operators, the backup pumps had been disengaged from the system by manual cutoff valves (failure 2). Since the light on the control panel indicating this condition was hidden by a maintenance tag, they assumed the backup pumps were operating as designed.

At this point, the reactor was automatically “scrammed”; that is, the control rods were lowered into the core to stop the nuclear chain reaction. However, even after the control rods are lowered, the core still emits a great deal of heat. However, operators observed soon after that the PORV light on the instrument panel had gone out, indicating that the valve was now closed when actually it had stuck in an open position (failure 3), causing coolant to be lost from the primary system. In response to the loss of coolant, the emergency injection water (EIW) system was activated. Operators did not recognize that coolant was being lost because the EIW had occasionally automatically turned itself on in the past when there was no leak. Operators observed via the control panel sensors that water level was rising and the pressure was dropping. These gage values were erroneous (failure 4). They turned off the EIW to avoid a condition in which the pressurizer “goes solid,” which they had been trained to avoid. Eight minutes into the incident, an operator finally realized that the secondary loop backup pumps were not connected and opened the valves to restore normal operation in the secondary loop. But, the water level in the reactor loop continued to drop due to the open PORV valve. About an hour and 20 minutes after the initial failure, the primary loop pumps began to shake violently due to cavitation (the

condition of pumping gas along with the fluid). Within the next 30 minutes, all of the pumps turned off. Without circulation, the core continued to heat up and convert more water to steam. By 6:15 am, the top of the core was exposed.

Soon after this, an operator from the next shift came on duty and noticed that the PORV discharge temperature was abnormally high and came to the conclusion that the PORV valve was actually open. The PORV's backup valve was finally closed to stop the leak. Although a complete meltdown had been avoided, it took another 13 hours before the temperature in the reactor core was under control. During this time period there was also an unexpected hydrogen explosion which fortunately did not breach the containment building. Although radiation leakage to the environment was minimal and no one was harmed by the incident, this disaster effectively doomed the nuclear industry in the United States.[15]

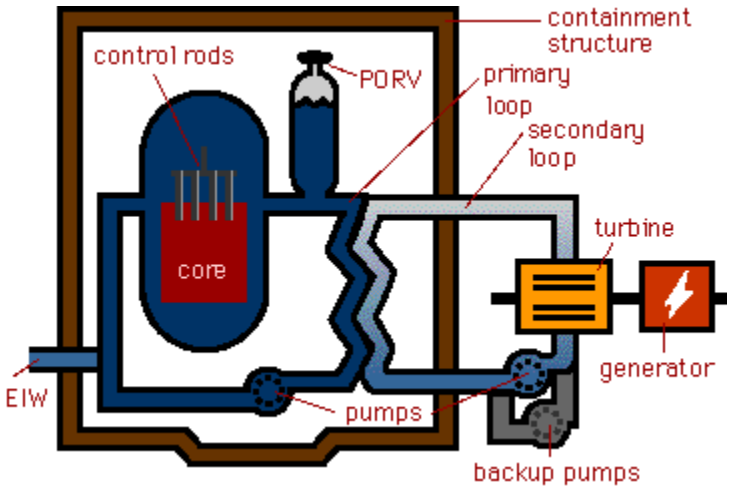

Figure 3. Nuclear Reactor Function. [16]

Although later reports placed blame on the operators involved, Perrow points out that the nature of this high risk technology is what really contributed to the near disaster. The lack of transparency of the reactor system forced operators to rely on incorrect or incomplete information in order to decide how to respond. The complexity of the control room instrumentation displays allowed critical information to go unnoticed. Expectations about how to fix the problem were not based on the correct mental models of the situation (e.g. because the EIW had operated in the past when there was no leak, it was incorrectly assumed that there was no leak).

Is nuclear power safe? Despite this incident, past data conclude that not a single fatality in the US has been associated with a nuclear disaster. But we need to recognize that we have relatively little operating experience with this technology. We would expect incidents to be few, but that does not reduce the potential for catastrophic harm in these highly complex and tightly coupled systems. There have been many documented trivial errors and failures in the nuclear power industry. If the assumption is that disasters are caused by the interactions of trivial errors, and that trivial errors are inevitable, then we need to devote extra attention to surveillance. Constant vigilance will need to be maintained to prevent nuclear failures from escalating into disasters. As a society, we need to determine whether the risks associated with nuclear power are worth the benefits. Balancing these risks against the risks due to global warming from other power generation sources is not a simple task.

5 Reducing Technological Risk

We must maintain a realistic view of our current situation: we know we can never eliminate the risks posed by technological systems, but by being diligent and comprehensive in our approach to design, we can significantly reduce the risk of future engineering disasters. The different sources of risk described in this paper can each be addressed by different techniques in the engineering education process and more generally.

An appropriate response to the risk potential induced by immoral choices at the individual level would include a commitment to the development of virtue and ethical judgment in our students. As engineering educators it is important for us to model ethical behavior in all aspects of our lives. This process is not just individual, but communal in nature. We need to emphasize the link between personal moral integrity and professional ethical standards for our students. Emphasizing spirituality and integrating faith perspectives can also help in motivating individuals to take professional standards seriously. Although the same faith perspectives are not generally shared among engineers and technology managers, engineering ethics codes generated by these groups emphasize the importance of developing the same character traits as many religious groups. For example, at my institution, which is committed to a Christian faith perspective, we challenge students to take the engineering code of ethics seriously because the requirements in the code are entirely consistent with the Biblical norms of the ten commandments and the need to "do justice and love kindness". On a professional level, we need to encourage distribution and enforcement of ethical codes among practicing engineers and engineering students. On a societal level, we need to support accountability for poor ethical choices in technology by adopting and enforcing appropriate laws and educating the public about the consequences of their choices related to how they interact with technology.

Many accident investigations conclude by assigning primary blame to the operator. We need to recognize, and help our students to recognize, that operator culpability is often used as an excuse to direct blame away from the designers and economic sponsors of the technology involved. A correct understanding of human immorality should allow us to recognize where people need to be held accountable, but we need to be clear that in many disasters, this category of reasons is not broad enough to completely explain the nature of the failure.

The responses to aspects of societal evil that contribute to technological risk need to be undertaken at the level of cultural and institutional change. We need a system of checks and balances surrounding technological innovation and maintenance that can reign in the worst tendencies of our current cultural situation. Market forces, along with adequate government regulation can both contribute to risk reduction. Professional engineering organizations can do their part by emphasizing the ideals to which the profession is committed. Engineering students need to be educated about the dangers of a technicistic worldview. Emphasizing the need for the humanities, as well as the real world contexts in which engineering design occurs, can be ways to counteract this tendency within the engineering curriculum.

Most importantly, engineering educators need to address the potential problems that human finitude introduces into the design of contemporary technological systems. We need to acknowledge the limitations of our mathematical models. This requires us to emphasize in every engineering science course that the equations we use are only incomplete representations of reality. We need to get in the habit of explicitly stating assumptions and application limits. We need to caution students against the over-reliance on computer models. Well-designed experiments are necessary to establish reliable predictions about a particular device, but with today's computer tools, it is often much easier for students to do simulation than to deal with "hardware".

Students need to undertake engineering design activities with due care. Diligence and clarity are required. Calculations need to be verified as correct, whether individually or by others. Henry Petroski describes this need in the following quote:

> "Engineers are not superhuman…That they make mistakes is forgivable, that they catch them is imperative. Thus it is the essence of modern engineering not only to be able to check one's own work, but also to have one's work checked and to be able to check the work of others."[17]

Creativity is a necessary requirement for reducing risk. Divergent thinking is necessary in order to anticipate modes of failure which have not been experienced in the past. This creativity should be directed towards developing inherently safe designs. Rather than focusing on the introduction of additional redundant safety systems, processes need to be redesigned in ways that eliminate risk potential. For example, eliminating the need for storage of MIC in the pesticide production process, either by substituting flow-through reactions or substituting a less toxic chemical, could significantly reduce the risk of the process. The techniques of robust design and Failure Mode and Effects Analysis (FMEA) should be included in the engineering curriculum to aid in this task.

Engineers need to focus on ways of reducing, rather than increasing, the complexity of our designs. In response to the continuing demand for increased product and system functionality and the need to add to current systems to achieve this functionality rather than completely rethinking the design, complexity tends to increase. We need ways of making complex systems understandable to designers and operators. This is often hindered by the proprietary nature of industrial technologies. Transparency of technology is also limited by the technological fluency of various members of society. Standardization of systems is highly desirable. For example, Southwest Airlines uses only one airliner (the Boeing 737) in its fleet, making it easier for pilots and mechanics to avoid mistakes and identify out-of-the-ordinary problems.

Engineering students need to be encouraged to approach technological design with humility and a respect for the seriousness of safety risks. Case studies of engineering disasters, similar to the examples considered in this paper, can be effective tools for promoting this awareness. The "Modern Marvels: Inviting Disaster" and "Engineering Disasters" video series produced by the History Channel[18] and the "Seconds from Disaster" programs[19] are good sources of case studies, as well as the "Inviting Disaster" website[20]. Of course, we do not want to scare students out of engineering by overemphasizing their responsibilities. Recognizing the different levels of contributing causes can help when discussing engineering failures to reassure students that the primary responsibility for design safety will not rest on them individually, but is a shared societal and professional calling.

6 Conclusion

The accident investigation for the Minneapolis bridge collapse is not yet completed, but current indications are that there may have been a serious design flaw in the original structure of the bridge. For a robust understanding of the causes of this disaster, we need to ask three questions corresponding to the categories described in this paper. 1) Were there immoral decisions made on the part of designers, builders, or users of this bridge that contributed to the disaster? At this point in time, investigations have not revealed any particular individuals who deliberately violated ethical obligations. 2) Were there violations of government responsibilities or effects of cultural pressures that contributed to the disaster? At this point, the investigation does not seem to point to failures in the bridge inspection system as being a cause. But, infrastructure maintenance is chronically underfunded in this country, and this may contribute to the risk. 3) Were there mistakes made by designers and/or operators, or did system complexity contribute to the disaster? At this point it appears that design calculations for the gusset plates were faulty. The bridge has

been updated several times since it was originally built, but it does not appear that this flaw was detected during inspections at any earlier points. Adding on to older structures to fill additional needs can be a risky activity when time is not taken to verify previous phases of work. Answering these questions completely will allow accurate understanding of the failures and guide us toward the steps which need to be taken to reduce similar risks for other bridges.

Correctly identifying the types of factors that contribute to engineering failures will allow us to practice and teach engineering in a way that emphasizes the "system" effects. It is not enough to emphasize that engineers need to have integrity and avoid immoral practices individually, although this is a necessary condition for avoiding engineering disasters. We also need to be aware that the way we practice design and the nature of the technological and cultural systems we interact with are contributors to some of the problems with technology. The categories described in this paper can provide an outline for accurately assessing the risks and the potentials of new technological developments. The categories can also serve as guidelines for including learning experiences in the engineering curriculum that prepare students for the safety issues they will need to deal with in their engineering careers. Some of these learning experiences must include elements typically emphasized in the liberal arts. The bad news derived from this robust understanding of technological failure is that there will be technological disasters in the future. The good news is that we can also be successful in preventing many of them if engineers work to understand technology and its effects more broadly.

References

[1] Wikipedia, the Free Encyclopedia, http://en.wikipedia.org/wiki/I-35W_Mississippi_River_bridge

[2] Wikipedia, the Free Encyclopedia, http://en.wikipedia.org/wiki/Homo_habilis

[3] Mitcham,C. *Thinking Through Technology: The Path Between Engineering and Philosophy*. University of Chicago Press: Chicago, 1994, p. 159 .

[4] Dym, C. and P. Little. *Engineering Design: A Project-Based Introduction, 2nd Edition*. John Wiley & Sons: Hoboken, NJ, 2004, p. 6.

[5] Schuurman, E. *Faith and Hope in Technology*. Clements Publishing: Toronto, Canada, 2003, p. 66.

[6] See Postman, Neil. *Technopoly: The Surrender of Culture to Technology*. Vintage Books: New York, 1992.

[7] Petroski, H. *To Engineer is Human: The Role of Failure in Successful Design*, Vintage Books: New York, 1982, p. 44.

[8] Martin, M. and R. Schinzinger, Ethics in Engineering, 4th Edition, McGraw-Hill: New York, 2005, p. 88.

[9] VanPoolen, L. "A Philosophical Perspective on Technological Design," *The International Journal of Applied Engineering Education*, Vol. 5, No. 3, pp. 319-329 (1989).

[10] See Tenner, E., *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*, Vantage Books: New York, 1996.

[11] Borgmann, A., *Technology and the Character of Contemporary Life: A Philosophical Inquiry*. University of Chicago Press: Chicago, IL, 1984. p. 41ff.

[12] See the National Society of Professional Engineers (NSPE) Code, http://www.nspe.org/ethics/eh1-code.asp

[13] *Aircraft Accident Report: Helios Airways Flight HCY522*. Hellenic Republic Ministry of Transport & Communications: Air Accident Investigation & Aviation Safety Board. English Translation posted November 2006

(http://www.moi.gov.cy/moi/pio/pio.nsf/All/F15FBD7320037284C2257204002B6243/$file/FINAL%20REPORT%205B-DBY.pdf)

[14] Data supporting this conclusion is described in "Understanding Technological Failure: Finitude, Fallennes, and Sinfulness in Engineering Disasters", *Proceedings of the Christian Engineering Education Conference*, June 2006, pp. 141-154.

[15] From the PBS website for "The American Experience: Meltdown at Three Mile Island" (http:/www.pbs.org/wgbh/amex/three/sfeature/tmihow.html)

[16] Ibid.

[17] Petroski, p. 52.

[18] DVD: *Modern Marvels: Inviting Disaster*. Episodes 1-4. A&E Television Networks, 2003. See also Chiles, James R. *Inviting Disaster: Lessons from the Edge of Technology*. HarperCollins Publishers: New York, 2002.

[19] http://channel.nationalgeographic.com/channel/seconds/

[20] http://www.invitingdisaster.com/

Acknowledgements:

Much of this material was originally presented at an Engineering Department seminar at Calvin College on September 28, 2005 and at the Christian Engineering Education Conference in June, 2006. The author is grateful for all of the discussion and suggestions generated by these events and to Calvin College for Sabbatical support in the fall of 2004, during which this work was initiated.