CHAPTER

7 Ethical Issues in Engineering Practice

Objectives

After reading this chapter, you will be able to

- Determine what ethical issues arise in engineering practice with regard to the environment
- Decide how engineering practice is impacted by computer technology
- Learn about ethical issues that arise in the course of research.

Between June of 1985 and January of 1987, at least six patients receiving treatment using the Therac-25 were exposed to high doses of radiation, leading to serious injury or death. The Therac-25 was a radiation therapy machine capable of irradiating tumors with either electrons or X-rays. Based on earlier versions of the machine, the Therac-25 was the first to incorporate significant computer controls.

The use of radiation for treating cancer is a well-established medical tool. Machines have been developed that deliver precisely controlled doses to tumors and the surrounding tissue without causing harm to healthy tissue in the patient. The Therac-25 was one of these machines and was based on earlier models produced by the same company. These machines had successfully treated thousands of patients. The problem with the Therac-25 was that the computer software used to control the machine and monitor the dose delivered to the patient was inadequate. Under certain circumstances, the software allowed the machine to be energized when it wasn't in the correct configuration. When this happened, patients could receive doses orders of magnitude larger than planned. Investigations in these cases determined that accepted standards for writing, testing, and documenting the software that controlled the Therac-25 had not been followed, directly leading to the accidents.

During the course of their careers, engineers use computers and software in performing design and analysis, or incorporate computers and software into the systems they design. Computers don't really create new ethical issues in engineering practice. However, computers do create new ways in which ethical issues confront engineers.

7.1 INTRODUCTION

There are many unique ethical issues that arise in engineering practice that may not be encountered in other professions. In this chapter, we will examine three important areas where engineers may encounter ethical concerns.

7.2 ENVIRONMENTAL ETHICS

One of the most important political issues of the late 20th and early 21st centuries has been environmental protection and the rise of the environmental movement. This movement has sought to control the introduction of toxic and unnatural substances into the environment, to protect the integrity of the biosphere, and to ensure a healthy environment for humans. Engineers are responsible in part for the creation of the technology that has led to damage of the environment and are also working to find solutions to the problems caused by modern technology. The environmental movement has led to an increased awareness among engineers that they have a responsibility to use their knowledge and skills to help protect the environment. This duty is even spelled out in many of the engineering codes of ethics.

Sometimes an engineer's responsibility for the environment is denoted with phrases such as "sustainable design" or "green engineering." These concepts incorporate ideas about ensuring that our designs do not harm the environment. By using sustainable design principles, engineers will help to maintain the integrity of the environment and ensure that our quality of life can be sustained. Sustainable design includes not only ensuring that a product has minimal environmental impact during its use, but also that it can be manufactured and disposed of without harming the natural world. These concepts have been incorporated into some of the engineering codes of ethics which specifically use the word "sustainable."

As concern about the environment has grown, ethicists have turned their attention to the ethical dimensions of environmentalism. In the late 1960s, an area of study called environmental ethics was formulated, seeking to explore the ethical roots of the environmental movement and to understand what ethics tells us about our responsibility to the environment.

Fundamental to discussing ethical issues in environmentalism is a determination of the moral standing of the environment. Our Western ethical tradition is anthropocentric, meaning that only human beings have moral standing. Animals and plants are important only in respect to their usefulness to humans. This type of thinking is often evident even within the environmental movement when a case is sometimes made for the protection of rare plants based on their potential for providing new medicines. If animals, trees, and other components of the environment have no moral standing, then we have no ethical obligations toward them beyond maintaining their usefulness to humans. There are, however, other ways to view the moral standing of the environment.

One way to explore the environment's moral status is to try to answer some questions regarding the place of humans in our environment. Do we belong to nature, or does nature belong to us? If animals can suffer and feel pain like humans, should they have moral standing? If animals have moral standing, how far does this moral standing then extend to other life forms, such as trees? Clearly, these questions are not easily answered, and not everyone will come to the same conclusions. However, there are significant numbers of people who feel that the environment, and specifically animals and plants, do have standing beyond their usefulness to humans. In one form, this view holds that humans are just one component of the environment and that all components have equal standing. For those who hold this

view, it is an utmost duty of everyone to do what is required to maintain a healthy biosphere for its own sake.

Regardless of the goal (i.e., either protecting human health or protecting the overall health of the biosphere for its own sake), there are multiple approaches that can be taken to resolving environmental problems. Interestingly, these approaches mirror the general approaches to ethical problem solving. The first approach is sometimes referred to as the "cost-oblivious approach" [Martin and Schinzinger, 2000]. In this approach, cost is not taken into account, but rather the environment is made as clean as possible. No level of environmental degradation is seen as acceptable. This approach bears a striking resemblance to rights and duty ethics. There are obvious problems with this approach. It is difficult to uphold, especially in a modern urbanized society. It is also very difficult to enforce, since the definition of "as clean as possible" is hard to agree on, and being oblivious to cost isn't practical in any realistic situation in which there are not infinite resources to apply to a problem.

A second approach is based on cost–benefit analysis, which is derived from utilitarianism. Here, the problem is analyzed in terms of the benefits derived by reducing the pollution—improvements in human health, for example—and the costs required to solve the problem. The costs and benefits are weighed to determine the optimum combination. In this approach, the goal is not to achieve a completely clean environment, but rather to achieve an economically beneficial balance of pollution with health or environmental considerations.

There are problems associated with the cost–benefit approach. First, there is an implicit assumption in cost–benefit analysis that cost is an important issue. But what is the true cost of a human life or the loss of a species or a scenic view? These values are difficult, if not impossible, to determine. Second, it is difficult to accurately assess costs and benefits, and much guesswork must go into these calculations. Third, this approach doesn't necessarily take into account who shoulders the costs and who gets the benefits. This is frequently a problem with the siting of landfills and other waste dumps. The cheapest land is in economically disadvantaged areas, where people don't necessarily have the political clout, education, or money required to successfully oppose a landfill in their neighborhood. Although dumps have to go somewhere, there should be some attempt to share the costs as well as share the benefits of an environmentally questionable project. Finally, cost–benefit analysis doesn't necessarily take morality or ethics into account. The only considerations are costs and benefits, with no room for a discussion of whether what is being done is right or not.

Given the complexity of these issues, what then are the responsibilities of the engineer to the environment? When looking at the environmental aspects of his work, an engineer can appeal to both professional and personal ethics to make a decision. Of course, the minimal requirement is that the engineer must follow the applicable federal, state, and municipal laws and regulations.

Professional codes of ethics tell us to hold the safety of people and the environment to be of paramount importance. So clearly, engineers have a responsibility to ensure that their work is conducted in the most environmentally safe manner possible. This is true certainly from the perspective of human health, but for those who feel that the environment has moral standing of its own, the responsibility to protect the environment is clear. Often, this responsibility must be balanced somewhat by consideration of the economic well-being of our employer, our family, and our community.

Our personal ethics can also be used to determine the best course when we are confronted with an environmental problem. Most of us have very strong beliefs

about the need to protect the environment. Although these beliefs may come into conflict with our employer's desires, we have the right and duty to strongly express our views on what is acceptable. An engineer should not be compelled by his employer to work on a project that he finds ethically troubling, including projects with severe environmental impacts.

In trying to decide what the most environmentally acceptable course of action is, it is also important to remember that a basic tenet of professional engineering codes of ethics states that an engineer should not make decisions in areas in which he isn't competent. For many environmental issues, engineers aren't competent to make decisions, but should instead seek the counsel of others—such as biologists, public health experts, and physicians—who have the knowledge to help analyze and understand the possible environmental consequences of a project.

7.3 COMPUTER ETHICS

Computers have rapidly become a ubiquitous tool in engineering and business. There are ways in which computers have brought benefits to society. Unfortunately, there are also numerous ways in which computers have been misused, leading to serious ethical issues. The engineer's roles as designer, manager, and user of computers bring with them a responsibility to help foster the ethical use of computers.

We will see that the ethical issues associated with computers are really just variations on other issues dealt with in this book. For example, many ethical problems associated with computer use relate to unauthorized use of information stored on computer databases and are thus related to the issues of confidentiality and proprietary information discussed in Section 6.2. Ethical problem-solving techniques used for other engineering ethics problems are equally applicable to computer ethics issues.

There are two broad categories of computer ethics problems: those in which the computer is used to commit an unethical act, such as the use of a computer to hack into a database and those in which the computer is used as an engineering tool, but is used improperly.

7.3.1 Computers as a Tool for Unethical Behavior

Our discussion of computer ethics will start with an examination of ways in which computers are used as the means for unethical behavior. Many of these uses are merely extensions to computers of other types of unethical acts. For example, computers can be used to more efficiently steal money from a bank. A more traditional bank-robbery method is to put on a mask, hand a note to a bank teller, show your gun, and walk away with some cash. Computers can be used to make bank robbery easier to perform and harder to trace. The robber simply sits at a computer terminal—perhaps the modern equivalent of a mask—invades the bank's computer system, and directs that some of the bank's assets be placed in a location accessible to him. Using a computer, a criminal can also make it difficult for the theft to be detected and traced.

It is clear that from an ethical standpoint, there is no difference between a bank robbery perpetrated in person and one perpetrated via a computer, although generally the amounts taken in a computer crime far exceed those taken in an armed robbery. The difference between these two types of robbery is that the use of the computer makes the crime impersonal. The criminal never comes face to face with the victim. In addition, the use of the computer makes it easier to steal from a wide variety of people. Computers can be used to steal from an employer: Outsiders can get into a system and steal from an institution such as a bank, or a company can use the computer to steal from its clients and customers. In these cases, the computer

has only made the theft easier to perpetrate, but does not alter the ethical issues involved. Unfortunately, the technology to detect and prevent this type of crime greatly lags behind the computer technology available to commit it. Those seeking to limit computer crime are always playing a catch-up game.

Similar computer ethics issues arise with regard to privacy. It is widely held that certain information is private and cannot be divulged without consent. This includes information about individuals as well as corporate information. Computers did not create the issues involved in privacy, but they certainly have exacerbated them. Computers make privacy more difficult to protect, since large amounts of data on individuals and corporations are centrally stored on computers where an increasing number of individuals can access it. Before we look at the ways that privacy can be abused by the use of computers, we will discuss the issues surrounding privacy and see what the ethical standing of privacy is.

By privacy, we mean the basic right of an individual to control access to and use of information about himself [Martin and Schinzinger, 2000]. Why is privacy an ethical issue? Invasions of privacy can be harmful to an individual in two ways. First, the leaking of private information can lead to an individual's being harassed or blackmailed. In its simplest form, this harassment may come in the form of repeated phone calls from telemarketers who have obtained information about an individual's spending habits. The harassment might also come in the form of subtle teasing or bothering from a coworker who has gained personal knowledge of the individual. Clearly, individuals have the right not to be subjected to this type of harassment. Second, personal information can also be considered personal property. As such, any unauthorized use of this information is theft. This same principle applies to proprietary information of a corporation.

How do computers increase the problems with privacy protection? This phenomenon is most easily seen by looking at the old system of record keeping. For example, medical records of individuals were at one time kept only on paper and generally resided with the individual's physician and in hospitals where a patient had been treated. Gaining access to these records by researchers, insurance companies, or other healthcare providers was a somewhat laborious process involving searching through storage for the appropriate files, copying them, and sending them through the mail. Unauthorized use of this information involved breaking into the office where the files were kept and stealing them or, for those who had access to the files, surreptitiously removing or copying the files. Both of these acts involved a substantial risk of being caught and prosecuted. Generally, these records have now been computerized. Although computerization makes the retrieval of files much easier for those with legitimate needs and reduces the space required to store the files, it also makes the unauthorized use of this information by others easier.

Ethical issues also arise when computers are used for "hacking." This has been widely reported in the newspapers and in popular culture, sometimes with the "hacker" being portrayed as heroic. Hacking comes in many forms: gaining unauthorized access to a database, implanting false information in a database or altering existing information, and disseminating viruses over the Internet.

These activities are by no means limited to highly trained computer specialists. Many hackers are bored teenagers seeking a challenge. Computer hacking is clearly ethically troublesome. As mentioned before, accessing private information violates the privacy rights of individuals or corporations, even if the hacker keeps this information to himself. In extreme cases, hackers have accessed secret military information, which has obvious implications for national security. Altering information in a

database, even information about yourself, is also ethically troubling, especially if the alteration has the intent of engaging in a fraud.

The issuance of computer viruses is also unethical. These viruses frequently destroy data stored on computers. In extreme cases, this act could lead to deaths when hospital records or equipment are compromised, to financial ruin for individuals whose records are wiped out, or even to the loss of millions of dollars for corporations, individuals, and taxpayers, as completed work must be redone after being destroyed by a virus.

Oftentimes, hackers are not being malicious, but are simply trying to "push the envelope" and see what they and their computers are capable of. Nevertheless, hacking is an unethical use of computers.

Copyright infringement is also a concern in computer ethics. Computers and the Internet have made it easy to share music, movies, software, and other copyrighted materials. A full discussion of the issues surrounding copyright is beyond the scope of this text. Briefly, copyright exists to protect the rights of authors, musicians, and others to profit from their creations. Copyright gives the creator the exclusive right to profit from his creation. The protection of copyright has become increasingly difficult as court cases related to music sharing websites such as Napster and other copycat websites have illustrated. Although computers make copyright violation easy to do and hard to detect, it is still illegal and unethical. If creators can no longer profit from their work—if their work is freely distributed without their consent—then the incentive to create will diminish, and this type of creative activity that enriches everyone's lives will diminish as well. There are those who advocate eliminating copyright altogether, mostly from the practical standpoint that modern technology makes copyright impossible to enforce and therefore useless. Nevertheless, copying music or software without the permission of the owner of the copyright is illegal and unethical.

7.3.2 Computers as an Engineering Tool

Computers are an essential tool for all engineers. Most often, we use computers for writing documents using a word-processing software package. We also keep track of appointments with scheduling software, use spreadsheets to make financial calculations, databases to keep records of our work, and use commercially available software to develop plans for how our projects will proceed. The use of these types of software is not unique to engineering—indeed, they are useful in various areas of business. Unique to engineering are two uses of computers: as design tools and as components integrated into engineered systems.

Computer Design Tools

Numerous software packages are available for the design of engineered devices and structures. This software includes CAD/CAM, circuit analysis, finite element analysis, structural analysis, and other modeling and analysis programs. Software also exists that is designed to aid in the process of testing engineered devices by performing tests, recording data, and presenting data for analysis. These all serve to allow an engineer to work more efficiently and to help take away some of the tedious aspects of an engineer's work. However, the use of this type of software also leads to ethical issues.

For example, who is responsible when a flaw in software used to design a bridge leads to the failure of the bridge? Is it the fault of the engineer who designed the bridge? Or is it the fault of the company that designed and sold the defective software? Who is at fault when a software package is used for a problem that it isn't

really suited for? What happens when existing software is used on a new and innovative engineering design that software hasn't yet been developed for?

These questions all have the same answer: Software can never be a substitute for good engineering judgment. Clearly, the engineer who uses software in the design process is still responsible for the designs that were generated and the testing that was done using a computer. Engineers must be careful to make sure that the software is appropriate to the problem being worked on, and should be knowledgeable about the limitations and applicability of a software package. Engineers must also keep up to date on any flaws that have been discovered in the software and ensure that the most recent version of the software is being used—software companies make patches and updates available, and engineers must check to make sure they have the most up-to-date version. Finally, it is important to verify the results of a computer-generated design or analysis. Sometimes it's a great idea to sit down with a piece of paper and a pencil to make sure that the output of a computer program makes sense and is giving the right answer.

Computer software can also give an engineer the illusion that she is qualified to do a design in fields beyond her expertise. Software can be so easy to use that you might imagine that by using it, you are competent in the area that it is designed for. However, it takes an expert in a field to understand the limitations and appropriate use of software in any engineering design.

Integration of Computers into Engineered Systems

Computers have also become a component of many engineered systems. For example, modern automobiles contain multiple computers, dedicated to specific tasks. Computers control the emissions and braking systems on automobiles and allow modern vehicles to operate more efficiently and safely. However, the ability to control aspects of system performance using software removes humans from the control loop. There are numerous examples of situations in which computerized systems malfunctioned without giving the operator any indication that a problem existed. In some cases, the operator was unable to intervene to solve a problem because the software design wouldn't allow it. It is essential when designing systems with embedded computers and software that engineers ensure that software is adequately tested, that humans can intervene when necessary, and that safety systems have enough hardware redundancy without relying solely on software to ensure the safe operation of the system.

7.3.3 Autonomous Computers

Other ethical concerns arise because of the increasingly autonomous nature of computers. Autonomy refers to the ability of a computer to make decisions without the intervention of humans. Some of the negative implications of this autonomy are chillingly spelled out in *2001: A Space Odyssey*, by Arthur C. Clarke, in which an autonomous computer responsible for running a spaceship headed for Jupiter begins to turn against the humans it was designed to work for. Certainly, there are applications for which autonomy is valuable. For example, manufacturing processes that require monitoring and control at frequent intervals can greatly benefit from autonomous computers. In this case, the autonomy of the computer has very little impact beyond the interests of the manufacturer.

Other autonomous computer applications are not so benign. For example, by the 1980s, computers were widely used to automate trading on the major U.S. stock exchanges. Some brokerages and institutional investors utilized computers that were programmed to sell stocks automatically under certain conditions, among them when

prices drop sharply. This type of programming creates an unstable situation. As prices drop, computers automatically start selling stocks, further depressing the prices, causing other computers to sell, and so on until there is a major market crash.

This scenario actually occurred on October 19, 1987, when the Dow Jones Industrial Average (a widely used market-price indicator) dropped by 508 points, a 22.6% drop in the overall value of the market. Interestingly, during the famous October 1929 stock market crash that launched the Great Depression, the percent drop in overall market value was only half of this amount. The 1987 crash was widely attributed to automated computer trading. Federal regulations have since been implemented to help prevent a recurrence of this problem.

Autonomy of computer systems has also been called into question with regard to military weapons. Many weapons systems rely heavily on computer sensors and computer controls. Due to the speed with which events can happen on a modern battlefield, it would seem valuable to have weapons that can operate autonomously. However, weapons systems operating without human intervention can suffer from the instability problems described with regard to the financial markets. For example, a malfunctioning sensor might lead a computer to think that an enemy has increased its military activity in a certain area. This would lead to an increased readiness on our part, followed by increased activity by the enemy, etc. This unstable situation could lead to a conflict and loss of life when really there was nothing happening [Rauschenbakh, 1988]. This problem is of special concern due to the implications for the loss of human life. It is clear from this example that although autonomous computers can greatly increase productivity and efficiency in many areas, ultimately there must be some human control in order to prevent disasters.

7.3.4 Computer Codes of Ethics

To aid with decision making regarding these and other computer-related ethics issues, many organizations have developed codes of ethics for computer use. The purposes of ethical codes and the way in which codes of ethics function are equally true for codes related to computer use. They are guidelines for the ethical use of computing resources, but should not be used as a substitute for sound moral reasoning and judgment. They do, however, provide some guidance in the proper use of computer equipment.

APPLICATION

CASES

Accidental Overdoses in Medical Radiation Therapy Systems

The Therac-25

The Therac-25 was a radiation therapy machine produced by Atomic Energy of Canada Ltd. (AECL), a Canadian company. AECL had previously collaborated with CGR, a French company, in the development of earlier versions of this machine. The Therac-25 was a dual-mode linear accelerator designed to deliver X-ray photons at 25 MeV, or electrons over a range of energies. The electrons are used to treat tumors relatively close to the surface, while the X-rays can be used therapeutically on deeper tumors. The Therac-25 was not the first radiation therapy machine produced by this partnership; similar machines, the Therac-6 and Therac-20, had been in use for a number of years. Although the previous Therac machines had utilized some level of computer control, they also relied heavily on hardware interlocks to ensure the safe operation of the machine. From the start, the Therac-25 was

designed to be controlled by software and did not incorporate the level of hardware safety devices found on the early machines.

The accidents involving the Therac-25 date back to the months between June 1985 and January 1987, comprising at least six known events of improper dosing of patients. There were 11 Therac-25 machines installed in the United States and Canada, with accidents occurring on both sides of the border. The six accidents involved overdosing of patients receiving radiation therapy for various types of cancer. Typical of these accidents was what happened to a patient at the East Texas Cancer Center in Tyler, Texas, in March of 1986. At the time of this accident, the Therac-25 had been in operation at this center for two years and had been used to treat over 500 patients. The patient in this case was being treated for a tumor in his back and was undergoing his ninth treatment with this machine. The prescribed treatment was to be 180 rads of 22 MeV electrons over a 10×17 cm^2 area of his upper back. As the treatment was started, the machine shut down, giving the operator an error code labeled "Malfunction 54." The meaning of this code was not identified in the manual that came with the machine. The machine also showed a "Treatment Pause" and an underdose, indicating that only about 3% of the requested dose had been delivered. Thinking that the treatment was incomplete, the operator told the machine to proceed, but it immediately shut down again. Because the video monitor was not working, the operator was unable to see the patient and didn't know that after the first dose, the patient had experienced what he described as an electric shock in his back. Knowing that something was wrong, he was attempting to get up when the second dose was delivered with the same painful effect. It was later estimated that the patient had received a total dose of between 16,500 and 25,000 rads, far higher than the 180 rads he was supposed to receive. In addition, the dose was concentrated in an area of approximately 1 cm^2. As a result of this malfunction, the patient developed symptoms of severe radiation poisoning and eventually died of complications related to the accident. The other six accidents were similar in nature, with similar consequences [Leveson and Turner, 1993].

The proximate cause of these accidents was a "bug" in the software. As the operators became comfortable with the software, they became quite proficient and fast at entering the data that set the type of treatment, dose, and energy. However, the hardware of the system required several seconds to reset when a command was changed on the computer keyboard. If the operator input the wrong information initially, quickly changed the settings to the correct ones, and hit the key that turned the beam on, the machine would go ahead and energize the beam, resulting in an incorrect dose being delivered. Basically, the software didn't wait for the hardware to reset before turning the beam on. Compounding the problem, there were no hardware interlocks available to shut the beam off when excessive doses were detected. The earlier versions of the Therac machines had this type of hardware safety system, but the Therac-25 relied on software to provide this protection [Casey, 1993].

In the wake of these accidents, investigations took place into the reasons for the malfunction of the machine. Two major areas of concern were identified:

- *Systems engineering.* In this complicated system, there was an almost exclusive reliance on the software to work correctly and ensure the safe operation of the machine. The lack of hardware safety systems was cited as one of the main problems with the Therac-25.
- *Software engineering.* Many software engineering errors were made during the development of the Therac-25, including inadequate documentation and testing of the software modules and the software.

Radiation Problems Continue

Although the problems with the Therac-25 occurred in the 1980s and were well known in the industry, medical radiation equipment used for cancer therapy continues to have problems, some leading to the deaths of patients. The root cause of these problems is the increasing complexity of the machines and the technologies used for radiation therapy. This complexity is manifested in software glitches and hardware failures and can contribute to human errors that can have devastating results.

A 2010 article in the *New York Times* [Brogdanich, 2010] described in detail two cases of severe patient injury caused by radiation therapy machines using linear accelerator technology. In both of these cases, the computer control system malfunctioned, leading to huge overdoses to the patients. In one case, a man suffering from oral cancer was treated using a linear accelerator system. In this machine, the beam shape and intensity was determined by a sophisticated collimator controlled by computer software. After three treatments, the physician, working with the health physicist responsible for implementing the treatment plan, decided to alter the dosing plan. As the health physicist input the new plan to the computer, the software "froze" and failed to properly store the new program. Because the new program wasn't stored properly, the computer instead directed the machine to leave the collimator wide open, not only greatly increasing the dose to the patient, but also allowing the dose to be given over a wide part of the patient's head rather than just to the cancerous area. This accident severely injured the patient, leading to a very slow and painful death from radiation poisoning.

Similarly, in the other case reported, a woman undergoing radiation treatment for breast cancer was overdosed. Her treatment was also being done using a linear accelerator system. In this machine, dosing was controlled using a wedge placed in the path of the beam to determine the intensity of the radiation and its location on the patient's body. In this case, the computer controlling the machine was inadvertently programmed to leave the wedge out of the beam, thus greatly increasing the dose received by the patient. In this case, the patient received a dose 3.5 times larger than planned during each of her 28 radiation sessions. The severe burns resulting from this overdose caused a large hole in the woman's chest that was painful and took months to heal. Ultimately, she died as a result of this overdose.

The *Times* article reported that New York is among the states with the most stringent requirements for reporting of medical radiation overdose incidents and maintains a database of these events. A review of the New York records indicated that 621 radiation treatment mistakes had been reported between January 2001 and January 2009, including incorrect dosing, irradiation of the wrong location on the patient, and even applying the treatment to the wrong patient. These mistakes were attributed to various causes including hardware malfunctions, computer software malfunctions, and various human errors.

When hardware and software malfunctions are the cause, what responsibility do engineers who designed these systems have for the accident? When designing any system with potential implications for human health and safety, engineers must be thorough in design and testing of the system, being especially concerned about anticipating potential failure mechanisms and designing to prevent these possibilities. In addition, fail-safe mechanisms should be incorporated into the design to ensure that failures are detected and do not lead to harm. For radiation therapy equipment, fail-safe means that the machine detects unsafe operating conditions and prevents patient irradiation until the problem is solved. Are engineers who design this sort of equipment also responsible for the human errors that led to

patient overdoses? Not all human errors can be anticipated and designed around. However, it is incumbent on a design engineer to design systems so that they are easy to operate and make it simple for operators to use properly. While an engineer cannot always anticipate all of the misuses, or all of the mistakes that might occur on an engineered system, it is essential that engineers try to anticipate these types of problems before they occur and design the system to minimize the possibilities that mistakes can occur.

Avanti Corp. vs. Cadence Design Systems

One of the most important assets a high-technology company can have is its intellectual property. Intellectual property includes new inventions, innovative ways of producing products, and computer codes. Intellectual property can be protected through the patent and trademark system of the federal government, or simply by maintaining "trade secrets." How computer software fits into the intellectual property protection scheme has been slowly developing. At first, software could not be patented, and it was unclear whether it could receive a copyright either. More recently, federal patent law has changed to allow software to be patented. Patenting does provide protection for intellectual property for a period of time, but in order to gain this protection, a software developer must divulge the code. This makes it easy for competitors to use ideas from the patent by designing around it. The best way to protect intellectual property is to keep it a trade secret.

Cadence Design Systems is the largest supplier of electronic design automation (EDA) products. Among other things, EDA products are used to do the layout of complex integrated circuits. EDA products are used by the various computer chip manufacturers. Avanti Corporation was a rival company in this field. In December 1995, the headquarters of Avanti was raided by police and FBI agents looking for evidence that trade secrets belonging to Cadence had been stolen by Avanti and incorporated into Avanti products. Specifically, Cadence claimed that up to 60,000 lines of code developed by its own software engineers had been used by Avanti. Cadence also filed a civil suit seeking damages from Avanti. In 1997, eight Avanti employees, including the chairman of the board, were indicted on criminal charges in the case. All of those who were indicted were former Cadence employees.

In order to understand the implications of this case, it is important to set it in the context of the high-tech industry in the United States. Both Cadence and Avanti were located in the Silicon Valley region of California. It is common for employees of one company to quit and move to a competing company just down the street. It is also common for a group of employees of a large company to leave and start a new company in the same field. It is often hard to determine the dividing line between skills and information learned at a former job and intellectual property belonging to your former employer.

The legal proceedings continued for several years, including a 1997 ruling by a court barring the sales of Avanti products containing the disputed computer code. The criminal cases culminated in a plea of "no contest" by seven of the Avanti defendants. (Charges against the eighth had already been dropped.) A no-contest plea is not an admission of guilt, but is an acknowledgment that if the case goes to trial, the defendant would likely be convicted. Five of the defendants faced jail time, one up to six years. All received various fines, some in millions of dollars. In a separate civil case, Cadence sought hundreds of millions of dollars in compensation from Avanti for the use of Cadence's intellectual property.

7.4 ETHICS AND RESEARCH

There are two major ethical issues related to research: honesty in approaching the research problem and honesty in reporting the results. The first relates to a state of mind essential to successfully performing research. This state of mind includes avoiding preconceived notions about what the results will be, being open to changing the hypothesis when such action is warranted by the evidence, and generally ensuring that an objective frame of mind is maintained. As we will see in the cases at the end of this chapter, this attitude is not necessarily easy to assume, but it is essential to producing useful research or test results. More will be said about this topic later in this chapter in the section on pathological science.

Results must also be accurately reported. Once an experiment or test has been performed, the results of the experiment must not be overstated, but rather an accurate assessment and interpretation of the data must be given. The environment that most researchers work in fosters temptations and rewards for overstating research results. Academic researchers must publish significant research results in order to get tenure at their universities. If an experiment isn't working out, it is tempting to "massage" the results to achieve the desired outcome. Even for researchers in industrial environments or faculty who are already tenured, the quest for fame or the desire to be the first with new results can be overwhelming and can lead to falsification of data. Often, the pressure to get a new product to market leads the test engineer to "fudge" data to qualify the product.

It is important to note the distinction between intentional deception and results or interpretations that are simply incorrect. Sometimes, results are published that, upon further research, turn out to be incorrect. This situation is not an ethical issue unless a clarification of the results is never presented. Rather, this issue indicates that great care must be taken before results are initially reported.

It is also important to ensure that proper credit is given to everyone who participated in a research project. Rarely is research performed by a single investigator working alone in her laboratory. Generally, there is participation by other people who should be acknowledged for their contributions such as discussions or guidance, construction of experimental apparatus, or substantial help with performing experiments or interpreting data.

It is tempting to think that fraud and deception in research are rare and only perpetrated by lower level scientists, but this perception is decidedly untrue. There are many examples of well-known and even Nobel Prize–winning scientists who have had lapses of ethical judgment with respect to their research. For example, Robert Millikan was a physicist from the University of Chicago who won the 1923 Nobel Prize in physics for experiments that measured the electrical charge of the electron. Studies of Millikan's unpublished data indicate that he excluded 49 of the 140 experimental observations from the paper that he published [Holton, 1978; Franklin, 1981]. However, in the paper, he stated that the published work contained all of the data. Inclusion of these data probably wouldn't have changed his conclusions, but would have made the result seem less certain and the experiment not as clearly definitive.

7.4.1 Analyzing Ethical Problems in Research

How can ethical issues relating to research best be analyzed? Perhaps the easiest means to determine the best ethical course in performing research and experiment is to consult the codes of ethics of the engineering professional societies. All of the codes include language requiring engineers to be honest in reporting the results of

work and assigning credit for work done. For example, the code of the American Institute of Chemical Engineers states that "members shall treat fairly all colleagues and coworkers, recognize the contributions of others," and "issue statements and present information only in an objective and truthful manner." These statements apply equally well to all professional activities of an engineer, including research, experiment, and testing.

Several ethical theories can be used to analyze issues involving research. Utilitarianism or rights and duty ethics can be applied to research, but it is perhaps easiest to examine research issues using virtue ethics. One of the virtues is honesty. Honesty facilitates trust and good relations between individuals, whereas dishonesty leads to doubts and misgivings about others. People rarely want to associate with those who they feel don't behave fairly and can't be trusted. Making false claims about the results of experiments is certainly a form of dishonesty. We should seek to enhance virtues such as honesty within ourselves and others, so virtue ethics clearly tells us that the inaccurate reporting of experimental results is unethical. Likewise, not giving credit to everyone who has participated in a project is dishonest, and virtue ethics indicates that this practice is unacceptable.

7.4.2 Pathological Science

As mentioned previously, self-deception is one of the biggest impediments to the successful completion of a research or experimental project. Self-deception in research is a frequent occurrence in many areas of science and has led to some notorious cases throughout history. Irving Langmuir, a well-known physicist working at General Electric Research Laboratories, coined a term for this phenomenon: "pathological science." He proposed the following six characteristics of pathological science [Langmuir, 1968]:

1. The maximum effect that is observed is produced by a causative agent of barely detectable intensity, and the magnitude of the effect is substantially independent of the intensity of the cause.

   This characteristic implies that it doesn't matter how close the causative agent is or how intense it is; the effect is the same. This practice, of course, goes against all known forces and effects.
2. The effect is of a magnitude that remains close to the limit of detectability; or, many measurements are necessary because of the very low statistical significance of the results.

   The problem here is that when things are at the edge of statistical significance or of detectability, the tendency is to discard values that don't "seem" right. To measure anything at the edge of detectability requires a lot of data. With a lot of data to work with, the measurements can be massaged to fit the conclusion that is being sought. In fact, what often happens is that data are rejected on the basis of their incompatibility with the preconceived theory, rather than on their true significance.
3. Claims of great accuracy.
4. Fantastic theories contrary to experience.
5. Criticisms are met by *ad hoc* excuses thought up on the spur of the moment.
6. Ratio of supporters to critics rises up to somewhere near 50% and then falls gradually to oblivion.

The term "pathological science" doesn't imply any intentional dishonesty, but only that the researcher comes to false conclusions based on a lack of understanding about how easy it is to trick yourself through wishful thinking and subjectivity.

This shows that a great deal of objectivity and care in the pursuit of research or testing is required. Drawing conclusions on very subtle effects is very tricky, and these conclusions should be confirmed by as many colleagues as possible. Ultimately, the goal of research is not publicity and fame, but rather the discovery of new knowledge.

APPLICATION

CASES

The City of Albuquerque vs. Isleta Pueblo Water Case

The city of Albuquerque, New Mexico, straddles the Rio Grande and is bounded on the north and south by two Indian pueblos (reservations). Several other pueblos are nearby. According to federal law, Indian tribes are sovereign nations with the wide-ranging ability to self-regulate but are subject to federal laws and some restrictions imposed by the states. Overall, however, their status is closer to that of an equal of state governments rather than a subordinate.

Isleta Pueblo is located on the Rio Grande, downstream from Albuquerque, and is contiguous to the Albuquerque metropolitan area, which contains close to 900,000 people. Traditionally, the Pueblo used water directly from the river for drinking during religious ceremonies. In more recent times, this practice has been difficult due to runoff entering the river—storm runoff is directly input to the river—and from treated sewer effluent placed into the river by Albuquerque. Similar effluent is probably discharged into the river by other municipalities farther upstream.

Of great concern to Isleta Pueblo is the concentration of arsenic in the river water. The Albuquerque sewage treatment plant puts water into the Rio Grande that meets all applicable Environmental Protection Agency (EPA) regulations, including the standard for arsenic concentration. Of course, the water placed into the river is not of drinking quality, since it is assumed that any municipality using river water for drinking must treat the water anyway.

Isleta Pueblo has used its sovereign status to try to enforce a stricter water quality standard for the water discharged by Albuquerque and seeks to bring the water quality to the point where it can be consumed directly from the river. This involves a standard for arsenic discharge that is roughly twice as stringent as the EPA regulations permit. The EPA has sided with the pueblo, citing federal law giving Indian reservations the right to set their own pollution standards. This case is analogous to the situation that might occur if Mexico decided that it wanted stricter regulation of the quality of water in the Rio Grande flowing from the United States south along the Mexican border.

The city of Albuquerque has argued that the pueblo's standards are too strict and are unnecessary, since the concentration of arsenic in the water that the city discharges into the river is lower than what naturally exists in the river upstream from Albuquerque, although this point is debatable. Albuquerque contends that the cost of meeting the standard would be prohibitive, approximately $300 million. The city also argues that the standard is a violation of the First Amendment's prohibition of government-established religion. Albuquerque pressed this case all the way to the U.S. Supreme Court, but the court turned down the consideration of Albuquerque's appeal in 1997 and thus will allow new EPA arsenic standards based on Isleta's requirements to stand. Albuquerque and other similarly affected municipalities are currently seeking federal government aid in meeting these new standards. Many other states and municipalities, especially in the west, are interested in this case.

The N-Ray Case

After the discovery of X-rays in the late 19th century, there was a great deal of interest among scientists in finding other similar types of rays. Many scientists joined this search in the hopes of achieving the fame that such a discovery would bring. In many ways, this scenario was similar to the frenzy in the scientific community in the 1980s upon the discovery of superconductivity at temperatures above the boiling point of liquid nitrogen. Many researchers dropped everything else they were doing and began searching for new materials with even higher superconducting temperatures, especially hoping to find one at room temperature. The search to find new rays was joined by a well-known French physicist, René Blondlot, at the University of Nancy. His case is discussed in depth in an interesting article published in 1980 by *Scientific American* [Klotz, 1980].

The apparatus used at the time for detecting such rays was the spark gap. This device consisted of two electrodes that were close enough together so that a spark developed between them in air when a large electric potential was applied between them. What we now know as electromagnetic radiation in the form of light or X-rays directed through the spark gap increased the ionization in the gap, increasing the current flow and the brightness of the spark. The brightness of the spark could be used to measure the intensity of the radiation present in the gap. Of course, by modern standards, this is a very crude means for detecting X-rays, but at the time, this method was state-of-the-art.

In order to see the change in brightness, care had to be taken in establishing the measuring environment. For example, the researcher had to stay in a darkened room sufficiently long so that his eyes would become dark adapted. Even then, the change in intensity of the spark could be very subtle, and care had to be taken to be honest in the assessment of the change.

In 1903, Professor Blondlot was working with gas discharges that produced the newly discovered X-rays. His previous experience was in the study of electromagnetic phenomena, and he was hoping to discover if X-rays were a wave or particle by determining if the X-rays could be polarized as visible light can be. Using a spark gap and an apparatus similar to the one that Roentgen had used to discover X-rays, Blondlot attempted to determine the polarization of X-rays by rotating the spark gap in the X-ray field. In his initial study, Blondlot discovered that, indeed, the spark gap became brighter when rotated to a certain angle with respect to the discharge tube. This was an important discovery.

Subsequent experiments indicated that the radiation impinging on the spark gap could be bent by a quartz prism. This feature was a major problem, since X-rays had already been shown by many scientists to be unaffected by lenses and prisms. The fact that the radiation he was measuring appeared to be bent by the prism convinced Blondlot that he had discovered a new form of radiation that he called N-rays (for the University of Nancy). He quickly published this work.

The reports of the discovery of a new type of ray set off a flurry of activity in other laboratories around the world, and Blondlot himself continued to study the phenomenon. Many discoveries were made about N-rays: Materials were found that transmitted them (metals, wood, mica, and quartz) and some that didn't transmit the rays (water and rock salt). Natural sources of N-rays were also discovered, including the sun and the human body. Despite the explosion of research on N-rays, there were also some doubts about Blondlot's findings. Many researchers outside France, including Lord Kelvin in England, had been unable to reproduce the results reported by Blondlot.

Prof. J. W. Wood of Johns Hopkins University was also unable to reproduce the results and traveled to Nancy to observe the experiments firsthand. In a paper published in *Nature*, he described the experiments that he had witnessed. Wood reported that when he observed the spark gap and someone placed a hand in the path of the N-rays, Wood didn't see the expected changes in intensity. Told that his eyes weren't sensitive enough, he exchanged positions with the French researchers and placed his hand in the path. The research team incorrectly reported whether his hand was in or out of the beam as they claimed to see changes in intensity. Wood reported that there was no correlation between the position of his hand and their reports of intensity.

Wood also observed a different experiment designed to spread the N-rays into a spectrum. The dispersion of the N-rays was accomplished using an aluminum prism and was observed using a thin phosphor strip painted onto a cardboard screen. Wood was unable to observe the variations in intensity from the phosphor that the French team claimed to see. Indeed, when Wood surreptitiously removed the prism from the apparatus, the researchers still claimed to see the effect! Wood was convinced after this incident that there were no N-rays and that the researchers had deluded themselves.

Publication of Wood's findings ended research into N-rays everywhere except in France. Blondlot responded to the criticisms and continued to present results of new, more controlled experiments. He even published a set of instructions for properly observing the phenomenon. For example, the instructions stated that the observer had to avoid gazing directly at the spark gap and instead had to look at it obliquely. The observer had to remain silent, avoid smoke, and had to look at the detector in the "way an impressionist painter would view a landscape" [Klotz, 1980]. Acquisition of this ability required a great deal of practice and might be impossible for some people. In other words, the key to the measurement was the sensitivity of the observer, rather than the validity of the phenomena. As more research was performed, it became clear even to the French that there were no N-rays.

The Case of Cold Fusion at Texas A&M University

On March 23, 1989, Stanley Pons and Martin Fleischmann of the University of Utah announced that they had produced excess heat in a tabletop electrochemical cell. The excess heat was presumed to be due to nuclear fusion, and the process was dubbed "cold fusion." Pons and Fleischmann's results were widely reported in newscasts and daily newspapers and led to great excitement among scientists around the world.

The apparatus used by Pons and Fleischmann was a fairly standard electrochemical cell. They found that when palladium electrodes were immersed in heavy water (water with the normal hydrogen atoms replaced by the heavier deuterium isotope) and an electric current run through them, heat far in excess of levels expected was produced. This heat production was attributed to the breakdown of the heavy water due to electrolysis, diffusion of the deuterium into the palladium, where the deuterium was thought to get to a density sufficient to initiate fusion, leading to the release of the excess heat.

Although Pons and Fleischmann were well-respected electrochemists, their results were treated with great skepticism by many scientists, especially those who had worked in conventional fusion and nuclear physics. This skepticism arose because, according to the contemporary understanding of the fusion process, the reaction of deuterium should produce copious amounts of tritium (another hydrogen isotope) and neutrons. Neither of these products was seen in the Pons–Fleischmann

experiments. The response of many of the believers in cold fusion to this criticism was that they had discovered some new form of fusion that didn't behave according to the old rules. Indeed, there were some claims of professional jealousy: Physicists who had worked for years to make conventional fusion practical would not be happy to be upstaged by chemists who couldn't possibly know anything about fusion. Despite the controversy, the potential benefits if this process proved to be real were so enormous that many researchers worldwide began setting up similar electrochemical cells in their laboratories and tried to reproduce the results. John Bockris at Texas A&M University was one of these scientists.

Stanley Pons and Martin Fleischmann, who started a frenzy in the scientific research community when they announced that they had discovered a way to control nuclear fusion in a tabletop electrochemical cell. AP/Wide World Photos.

Bockris's research group built electrochemical cells like those of Pons and Fleischmann and set out to verify the Utah work. By April 22, 1989, this group had observed a surprising result. A graduate student working with Bockris, Nigel Packham, had removed samples of the electrolyte from three of the cells in the laboratory and took them to another campus building, the Cyclotron Center, for tritium measurements. Two of the three samples were "hot," containing 109 tritium atoms/ml, an amount far in excess of the expected background level. Subsequently, tritium was detected in four more cells.

When this work was reported at scientific meetings, there was immediate concern, since the data were too amazing. More work was performed, designed to control the experimental conditions more carefully, including work by other researchers at Texas A&M. For example, Kevin Wolf, a nuclear chemist, ran a cell in front of neutron detectors in his laboratory, hoping to find the telltale sign that should accompany tritium production. No neutrons were detected, although tritium did appear in the electrolyte when tested. Packham also performed an experiment in which electrolyte samples were taken at four different intervals over 12 hours while the cell was running. At the beginning of the experiment, tritium was at background levels. Two hours later, it was slightly above the background level. A few hours later, the level had climbed greatly to 5 trillion atoms, and at 12 hours it had climbed to 7.6 trillion atoms [Taubes, 1990]. Although these data seemed to confirm that tritium was being produced in the cell, skeptics also pointed out that this result was consistent with someone "spiking" the sample with tritium sometime toward the middle of the experiment. Indeed, there was a supply of tritium stored in the laboratory.

In response to these allegations, Bockris and his team failed to take steps to ensure that intentional spiking couldn't occur. Offers to place the experiment in the locked laboratory of colleague Charles Martin, another electrochemist, were refused, and the bottle of tritiated water in the laboratory was not locked up or thrown away. While Bockris continued his work, Wolf and Martin continued their own similar studies with the same type of cell used by Bockris. Martin even took the precaution of taking cells home to ensure that there would be no sabotage. Martin's cells never showed signs of tritium.

In late September, after nearly three months with no results, two more cells turned up with tritium. The discovery of new cells containing tritium coincided with a scheduled visit from officials of the Electric Power Research Institute (EPRI), which had funded some of the research at Texas A&M. This incident and coincidences with other visits from funding sources cast more suspicion on the tritium results.

On November 27, 1989, Packham, who had not been involved with this work for several months, decided to test samples from two previously untested cells with titanium electrodes. These samples proved to be hot as well. The coincidence was too much for several of the workers in the laboratory. They took their concerns to Bockris, who dismissed their claims. These scientists subsequently went to other laboratories or sought employment outside the university.

Through most of the controversy, the university had taken a hands-off approach. There had been inquiries of Bockris as to his results and why they appeared so anomalous. However, the university allowed the situation to continue. In June 1990, Gary Taubes published an article on this situation in *Science*. The negative publicity, especially the statements that the university appeared to be doing nothing, prompted an internal investigation by the university. The three-member panel appointed by the university concluded that intentional spiking of the samples could not be ruled out, but that it was more probable that the results were due to inadvertent contamination

or other unexplained problems with the measurements. The panel did find that there were lapses in proper scientific procedure caused by the excitement surrounding the study of a new discovery that was receiving so much media attention. These lapses included categorizing experiments that supported the hypothesis of cold fusion as "successful" and those that didn't support it as "failures" [Pool, 1990].

Unable to reproduce the Pons–Fleischmann results, many researchers stopped their investigations of cold fusion. Funding for this work has dried up, although there are still a few people who believe in the phenomenon and continue to study it. Fraud was certainly a possibility at Texas A&M, although it is unclear who was responsible if this is true. However, all of the researchers were responsible for performing their experiments in an objective manner. In the face of charges of fraud, steps should have been taken to ensure that spiking was not possible. The reputations of senior scientists as well as of students and the university were tarnished by this episode.

Ghostwriting of Research Articles

A great deal of attention has been focused in recent years on conflict of interest in research. At its best, research is supposed to be unbiased, and results should be reported truthfully. Since researchers are human, it is sometimes difficult to maintain the detached and open attitude that is required. Nowhere is this more difficult than in pharmaceutical research. Much of the research on new drug therapies is funded by the federal government through agencies such as the National Institutes of Health (NIH). However, a substantial fraction of the research taking place in universities is funded by pharmaceutical companies, leading to substantial concerns about bias in performing research and reporting of the results. In response to this, most research papers in this area explicitly mention that a pharmaceutical company is funding the work, or disclose any conflicts that the researchers performing the work might have.

A new area of ethical concern has arisen lately with reports of "ghostwriting" of research articles by pharmaceutical companies who sponsor the research. A 2009 article in *The Chronicle of Higher Education* [Basken, 2009] described two cases where researchers incorporated significant amounts of material written by employees of drug companies into their own research papers. In one of these cases, it appears that DesignWrite, a company hired by a pharmaceutical manufacturer, provided a university researcher with extensive background information for the literature review in the paper and drafted a summary of the researcher's existing data. The final paper that was published did not acknowledge the contributions made by DesignWrite to the work. *The Chronicle* article also cited a study presented at a medical conference that indicated that at least 11% of the articles published recently in *The New England Journal of Medicine*, a very prestigious medical journal, had substantial and often unacknowledged contributions from ghostwriters.

What are the ethical issues here? Most significant is the potential for introduction of bias into a research article when the author has substantial financial ties to the drug industry. In writing a research paper, the author makes decisions about what data to include and what to omit, how to present the data, and what conclusions should be presented. If one of the main contributing writers is paid directly by a drug manufacturer who has a stake in the outcome of the research, the objectivity of the reporting of the research is called into question. An ethical issue also arises when someone who made significant contributions to the writing of the article is not acknowledged. Many people, including a U.S. senator, are calling for an end to this practice, and are urging NIH to develop stronger guidelines and new enforcement mechanisms to prevent ghostwriting of research articles in the future.

PROFESSIONAL SUCCESS

FALSIFYING EXPERIMENTAL RESULTS

Experimental work is an important part of an engineering student's education. It is no surprise that ethical issues often arise in the course of laboratory work. Most ethical issues in experimentation relate to honesty in reporting results. For example, it is often tempting to "massage" data to get the desired result. Or sometimes, it seems easier to "dry run" an experiment by recording measurements and results in your laboratory book even though you haven't actually performed the experiment. Fundamentally, these are very similar to cheating.

How do you decide what is ethical in experimentation? It is easiest to look at ethical issues related to experimentation using virtue ethics. Honesty is a virtue that should be fostered within ourselves. So, virtue ethics tells us that the utmost care must be taken to ensure that experiments are performed carefully and the results are reported honestly.

KEY TERMS

Computer ethics Ethics in research Pathological science

REFERENCES

Wayne Leibel, "When Scientists Are Wrong: Admitting Inadvertent Error in Research," *Journal of Business Ethics,* vol. 10, 1991, pp. 601–604.

Alexander Kohn, *False Prophets*, Basil Blackwell, Oxford, 1986.

Gerald Holton, "Subelectrons, Presuppositions, and the Millikan-Ehrenhaft Dispute," *Historical Studies in Physical Sciences,* vol. 11, 1978, p. 185.

A. D. Franklin, "Millikan's Published and Unpublished Data on Oil Drops," *Historical Studies in Physical Sciences,* vol. 58, 1981, p. 293.

Irving Langmuir, "Pathological Science," in R. N. Hall (ed.), General Electric Research and Development Center Report No. 68-C-035, April 1968.

Boris Raushenbakh, "Computer War," pp. 45-52 in *Breakthrough: Emerging New Thinking*, Anatoly Gromyko and Martin Hellman (eds.), Walker, New York, 1988.

Roland Schinzinger and Mike W. Martin, *Introduction to Engineering Ethics*, McGraw-Hill, New York, 2000.

Medical Radiation Accidents

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

Steven M. Casey, *Set Phasors on Stun, and Other True Tales of Design, Technology, and Human Error*, Aegean Publishing Company, Santa Barbara, CA, 1993, p. 13.

Walt Brogdanich, "A Lifesaving Tool Turned Deadly," *The New York Times*, Sunday, Jan. 24, 2010, National Edition, Front Section, p. 1, column 2.

Avanti vs. Cadence

Richard Goering, "Avanti Pleads No Contest," *EE Times*, May 28, 2001, p. 1.

Isleta Pueblo Water

Tania Soussan, "8 States Watching Water Quality Suit" *Albuquerque Journal*, Section C, June 24, 1997, p. 1.

Tania Soussan, "Isleta's Water Demands Upheld" *Albuquerque Journal*, Section A, November 11, 1997, p. 7.

N-Rays

Irving M. Klotz, "The N-Ray Affair," *Scientific American*, May 1980, vol. 242, no. 14, pp. 168–170.

Cold Fusion

Articles in *New York Times*, March 24 and 28, 1989, and numerous subsequent articles. Also, this story was widely reported at the same time in many daily newspapers across the country.

Robert Pool, "Cold Fusion at Texas A&M: Problems, But No Fraud," *Science*, December 14, 1990, vol. 250, pp. 1507–1508.

Gary Taubes, "Cold Fusion Conundrum at Texas A&M," *Science*, June 15, 1990, vol. 248, pp. 1299–1304.

Ghostwriting of Research Papers

Basken, Paul, "Ghostwriters Haunt the Integrity of Medical Journals," *The Chronicle of Higher Education*, September 18, 2009, p. A10.

PROBLEMS

7.1 Write a code of ethics for computer use by engineers.

7.2 Is there an ethical obligation to ensure that the information you post on your Internet website is accurate and true? Or is it up to the Web user to be discriminating and to realize that some material might not be accurate?

7.3 There is much in the news about the use of the Internet to disseminate pornographic images, especially in the context of the availability of this material to children. What ethical issues do "cyberporn" and efforts to limit it raise? Do employers have the right to fire employees who access pornography on their computers at work?

7.4 Many desktop computers come with games already installed on them. In addition, there are many websites where users can download games onto their computers. Is it alright to play computer games at work? How about during lunch? After hours?

7.5 Should computer and software designers be concerned about the possible abuse of their products? Should designs incorporate methods for preventing the misuse of computers?

7.6 Is it acceptable for employees to use their computers at work to send and receive personal e-mail?

7.7 There has been some discussion of having the federal government maintain a computer database of medical information on everyone in the United States. Some medical researchers feel that such a database might save lives by allowing access to a larger base of medical records for research purposes. Certainly, this database would make certain legitimate government functions more efficient. Is this a good idea?