

TEACHING ETHICS IN THE ENGINEERING DESIGN PROCESS: A LEGAL SCHOLAR'S PERSPECTIVE

Vincent M. Brannigan *

Abstract - Engineering ethics are a critical "gap filler" in the regulation of technology. Engineers, as "professionals", are given professional autonomy in promoting risky activities, based on a promise that they will act in the public interest. Both regulation and liability put constraints on the design process, but often leave gaps that must be filled by ethical precepts. The conflict between the public's interest and the private interest of the engineer is often most acute in the acceptance or rejection of relatively rare risks with the greatest uncertainty of injury. Rare risk of catastrophic injury can fall "under the radar" of regulatory systems, or technological advances may make regulatory systems obsolete. A key ethical problem can be described as "design process" failures where engineers wrongfully assume that another party will cope with a risk. Engineers must be taught to recognize and deal with ethical problems in product design. In particular reliance on regulatory approval may be insufficient. Design processes that actually **Hold paramount** the public safety must be the benchmark for engineering ethics.

Index Terms Ethics, Liability, Regulation, Design.

ETHICS IN ENGINEERING DESIGN

Technology represents the potential for both benefit and harm to society. There is tension between the desire for beneficial technological innovation and the need for social control to prevent innovations from causing harm, especially personal injury. This paper is designed to reflect both an analytical description of the ethical implications of legal and engineering concepts of safe engineering design, and illustrate the teaching technique used to convey these concepts to students in two separate courses taught at the University of Maryland's Clark School of Engineering:

ENES 100 Introduction to Engineering Design is taken by all engineering students in their first year. A two-hour ethics module includes many of the examples described in this article.

ENES 435 Product Liability and Government Regulation is a senior level technical elective open to all students in the school. The course concentrates on the social control of the design process. Ethics is analyzed continuously through the course and particularly in the advanced issues noted below.

Safety is the prevention of unintentional personal injury. Even setting aside weapons and other products that are supposed to be dangerous, engineered products can clearly kill or injure large numbers of people either "all at once" or one at a time. There is no automatic relationship between the benefit a technology can create and the harm it can cause. Since the developers and users of technology may not internalize the full costs of injuries, they may even have little incentive to avoid potentially harmful innovations.

A product can be dangerous for many reasons. Engineered products can have substantial kinetic or potential energy, can use flammable or toxic materials, can fail to protect an individual against an environmental hazard or can even be misused as a weapon. Injuries occur, not normally to the engineer or even the client, but to members of the public. The safety of engineered products has therefore always been a matter of social, not merely private concern. There have been two fundamental methods used by society to control the hazard of engineered products. The first approach was to use the power of the legal system to require engineers to make safe products. In one of the oldest written codes of law, the Babylonian king Hammurabi wrote "if a building collapses killing the owner then the builder shall be put to death". The legal system demands safety both directly through regulation and indirectly through product liability and professional negligence. [1]

While regulations have been widely used, since W.W. II a professionally oriented "self-regulatory" approach has gained ground. The core has been the development of a code of professional engineering ethics oriented towards safety in the design of products.

Professional Ethics

The existence of a code of professional ethics is one of the hallmarks of "professionals" (at least in any sense other than being paid for the work). Professions have traditionally involved advanced training, and some kind of peer control over membership and practice. Professions are accepted because of their importance to the public interest. Professional ethics are part of the peer review defining behavioral expectations for the professionals. Arguably the oldest formal statement of professional ethics is contained in versions of the Oath of Hippocrates. The Hippocratic oath defined the relationship between a physician and a patient. From ancient times physicians have been expected to put the patient's interest above the physician's. This oath made clear that a physician is not merely a practitioner in

* Department of Fire Protection Engineering, University of Maryland College Park Maryland 20742 firelaw@umd.edu

“business” selling medical services to customers. Often summarized in the epigram “Primo non nocere” the oath enjoins the physician to “above all, do no harm”.

Attorneys have been bound by similar codes of ethics for hundreds of years. Being “called to the bar” created obligations not merely to the client, but to the public through the court system. Attorneys who violate their ethical responsibilities can be and are disbarred.

Professional Duties to the Public

These ethical obligations of attorneys and physicians do not change simply because of the professional’s employment status. Whether working for free, for a salary, or paid by a third party for a given matter, the ethical obligations of the attorney or physician do not change. An attorney or physician is at all times required to put the interest of the “protected person” above their own personal interest or the interest of the person paying them. A corporate attorney can owe a professional duty to the stockholders, not the management who pays the fees. The canons for attorney’s make this explicit:

c) A lawyer shall not permit a person who recommends, employs, or pays the lawyer to render legal services for another to direct or regulate the lawyer's professional judgment in rendering such legal services.[2]

ABET’s Canons of Ethics ,similarly require engineers to put the public interest first:

“The engineer who makes the decision to “blow the whistle” will in many instances be faced with the loss of employment. While we recognize this sobering fact, we would be ignoring our obligation to the Code and hence to the engineering profession if, in matters of public health and safety, we were to decide otherwise”[3]

The “self awareness” of engineers as members of a profession with direct obligations to the public seems to vary across engineering fields. This in part due to the reality that engineers do not have a single professional organization. Only some engineers are licensed as “professional engineers” (PE) and many employers regard engineering as merely a form of training rather than as a distinct profession. Civil, Mechanical and Fire Protection Engineers routinely seek and showcase their PE status. In return many state and local building regulatory departments will only accept plans stamped or sealed by “professional engineers”. On the other hand, large firms employing engineers in aerospace, chemical, computer and similar industries do not seem to focus on PE status in quite the same way. The same variation may affect their Canons of Ethics. This article will use ABET’s Canons as a common expression, recognizing that variations exist across engineering fields.

Unquestionably the analogy of the ethical obligations of engineers to those of physicians and attorneys is complex. Unlike attorneys, ethical lapses by engineers can often result in death or serious injury. Unlike physicians (whose patients are the person at risk), engineers normally design products and systems, rather than deal with individuals. Injuries can even be caused many years later. In addition, hazardous products or systems are designed by the engineer, but are typically built by the engineer’s “clients”. As a result an engineer’s “client” does not stand in the same position as an attorney’s client or a physician’s “patient”. The person who needs protection is not normally part of the contractual relationship. In a few rare cases the client is in fact the person at risk. If the person who is actually at risk is in a position to evaluate the risks and benefits of a product then the engineer may be able to discharge any ethical obligation by fully disclosing to that person the risk and alternatives. However it is inherent in the nature of engineered products that such situations will be rare. The client, in effect, is normally a “part of the problem”, rather than the person being protected. The engineer’s ethical obligation is therefore to prevent the client from using the engineer’s skill to injure the public.

The focus of engineering ethics education is therefore on protection of the public safety, rather than the client’s interest. Engineers can claim to be “professionals” to the extent that they accept the obligation to protect the “public” from their actions. Such obligations are not unique to engineers. Physicians who treat patients with reportable “public health” conditions owe a duty to the public. Attorneys likewise owe a duty to the public. For example attorney client confidentiality does not apply to communications involving future bodily harm.

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary: (1) to prevent reasonably certain death or substantial bodily harm:[2]

For the purpose of this article it is assumed that all true professionals share an obligation to protect the public even at the expense of their own economic well being, and often in direct opposition to the client’s narrow economic interest.

HOLD PARAMOUNT

The bedrock principles of engineering ethics that affect the design of products are found in the ABET Canons of Ethics.

Fundamental Canons

Engineers, in the fulfillment of their professional duties, shall:

- 1. Hold paramount the safety, health and welfare of the public.*
- 2. Perform services only in areas of their competence.*

These Canons acting together require engineers to both fully understand the products they are designing and make sure those products meet a high standard of public safety. Some disciplines articulate enhancements to the Canons. The ASME's are typical and state:

Engineers shall recognize that the lives, safety, health and welfare of the general public are dependent upon engineering judgments, decisions and practices incorporated into structures, machines, products, processes and devices.

Engineers shall not approve or seal plans and/or specifications that are not of a design safe to the public health and welfare and in conformity with accepted engineering standards.

Engineers shall conduct reviews of the safety and reliability of the designs, products, or systems for which they are responsible before giving their approval to the plans for the design.

Whenever Engineers observe conditions, directly related to their employment, which they believe will endanger public safety or health, they shall inform the proper authority of the situation. [4]

These Canons, and similar ones impose a high standard of responsibility to the public. However, it is not obvious what it means to "hold paramount" public safety. Students (and practicing engineers) are often frustrated that no one will say how safe to make a product. How does the engineer balance benefits and risks in modern engineered products?

Some authors have declared that safety should never be allowed to interfere with "functionality". Brickman and Barnett claim that **"safeguards that interfere with functional specifications must be rejected"** and that such a design philosophy is in accordance with the Canons of Ethics, "the Engineering code of Ethics ...does not allow functionality to be compromised in the design process". The argument is based on a claim that the "welfare" protected by the Canons includes the economic well being which would be violated if safety was allowed to overcome functionality. This argument fails to appreciate the distinction between the "private" interest the client has in functionality and the "public" interest in safety. Engineering ethics would mean little or nothing if the private interest in functionality were to be held **"inviolable"** against the public safety as Brickman and Barnett assert. [5]

Efficient Level of Safety

The question remains, to what level of safety should we design products? A standard description of the "efficient" level of safety in a desirable product is a level that minimizes the joint sum of injuries and injury avoidance

activities. Such an analysis looks at the cost of safety and adds it to the cost of injury and sets the level of safety at the level with minimizes the joint cost. The "efficiency" formula has several problems. The first is simply valuation. While the cost of injury avoidance is easy to analyze the benefit in terms of injuries avoided does not lend itself to easy quantification. How much is a leg or a life worth? As a teaching technique engineering students are asked to write down how much they would ask to be paid to sell their head of hair. (Students with religious objections are excused.) Answers obtained have routinely ranged from \$1 to \$50,000. Students quickly conclude that valuation of injuries is a socio/political choice.

Second, the "efficient" level of safety (like the Brickman/Barnett philosophy), is relatively insensitive to the "distributional equity" issues involved when public costs are weighed against private benefits.

The third problem deals with rare risks. The efficiency formula does not work well with rare injuries with high uncertainties. When the probability of injury is not known to a reasonable level of certainty, quantitative estimates of the risk may be based on assumptions of dubious validity.

As a result, while the efficient level of safety is a starting point for analyzing the socially desired level of safety it is both hard to put into practice and may mask fundamental inequities and analytical errors.

LEGALLY DEFECTIVE PRODUCTS

Legal actions including product liability and product recalls can offer some guidance to an engineer trying to solve the ethical issues the design of a product. The guidance is imperfect since standards for product liability and product recall are not exactly the same as the ethical obligation of the engineer. Legal requirements may depend on unusual statutory or common law obligations or defenses. However they can be a start and make excellent classroom examples.

Case 1 Aluminum Baseball Bats With Rubber Knobs

Baseball bats have knobs on the end to allow the hitters to keep control of the bat and avoid hitting the pitcher. Early aluminum baseball bats were deliberately engineered without rigid knobs on the ends of the bats. Instead the knob was part of the soft rubber grip and like all rubber could deteriorate in the sunlight and sand of the ball field. The bats were designed for use by little leaguers and other children and had simple plastic stickers that indicated that damaged grips could "cause injury". The manufacturers sold replacement grips. The Consumer Product Safety Commission forced the recall of these bats over strenuous objection by the manufacturer.

The bat case is very useful to demonstrate the problems of engineers who blindly follow management without conducting **"reviews of the safety and reliability of the designs, products, or systems for which they are responsible before giving their approval to the plans for**

the design”. Students are often horrified by the idea that major manufacturers would deliberately create a product with a known risk of injury to children.

Case 2 Dalkon Shield IUD

The Dalkon shield involved an intra uterine contraceptive device (IUD) with a safety flaw. Like most IUDs the Dalkon Shield had a “tail” which extended from the contraceptive device in the uterus to the vaginal canal. The tail assured the user that the device had not been expelled. However unlike prior IUDs that had a tail formed with the IUD and was effectively a nylon monofilament, the Dalkon shield tail was a “multi filament” which provided a protected path for bacteria to enter the uterus and cause pelvic inflammatory disease. An engineer spotted the problem in the pre production stage and brought it to the management’s attention. However, nothing was done, the device went into production, and thousands of women were injured. While the engineer quit he did not “blow the whistle” on the product. The ASME now requires such whistle blowing.

Whenever Engineers observe conditions, directly related to their employment, which they believe will endanger public safety or health, they shall inform the proper authority of the situation

The ASME canon requires products to comply with both safety standards and government regulations:

Engineers shall not approve or seal plans and/or specifications that are not of a design safe to the public health and welfare and in conformity with accepted engineering standards.

The ethical requirements clearly involve a “dual track” approach. The design must be in compliance with accepted engineering standards and it has to be safe.

COMPLIANCE WITH REGULATORY STANDARDS

Many engineered products must comply with regulations before being put on the market. As previously noted compliance is not automatically sufficient, since the dual track approach requires both safety and compliance. However engineers in some environments may believe that all ethical requirements are satisfied if the product simply complies with regulatory standards.

“Compliance” with regulatory standards is itself a very complex problem, since regulatory standards vary from comprehensive tightly restrictive controls that allow almost no regulatory discretion, to very open imprecise requirements that allow a wide range of technologies as long as they are “approved” by the regulatory authority. The terms “prescriptive” and “performance” regulation are often used to describe these varying types of regulation, although they

clearly exist on a continuum. Whenever someone claims that a product “complies” with regulatory standards it is vital to know what type of regulation is involved.

The ability to properly regulate a developing technology depends heavily on the ability of regulators to anticipate, recognize and react to the phenomena of technological innovation itself. [6] Inadequacies in regulatory structures can easily permit the introduction of dangerous technological innovations that fail to comply with social safety goals.[7] When innovative technology confronts inadequate regulatory systems the result can be disaster. The problem exists in both prescriptive and performance regulation. Regulation requires flexibility to properly promote innovation. Prescriptive regulation can both inhibit desirable technology or even allow dangerous technology that nominally but not actually complies with the intent of the regulation, and performance requirements can be created that inadequately measure the hazard of a new technology. This potential gap is one of the strongest arguments for both Codes of Ethics and professional peer review.

Case 3 RMS TITANIC

The RMS TITANIC complied with prescriptive standards for lifeboats, but chief engineer Wilding was also involved as an advisor to regulators who proposed weakening lifeboat standards that he already considered inadequate. It would appear that Wilding signed off on the proposed reduction on the assurance that “big ships would fit more boats than were required by the Board of Trade”. Despite his expressed concern, in the end he designed TITANIC with many fewer lifeboat places than persons on board. When TITANIC was completed she carried only the boats required by regulations that Wilding stated were inadequate.

What is even worse is that TITANIC not only had insufficient lifeboats for the number of persons on board, but it could not even properly fill and man the lifeboats it carried. When the ship sank there were hundreds of unfilled spaces and as a result, hundreds of extra lost lives. The problem was an inadequate design analysis. Lifeboats are part of a rescue system that requires both boats and skilled manpower. Innovations that permitted the TITANIC’S great size did not require a proportionate increase in the seamen normally used to handle the boats. Additional boats were not provided because designers believed insufficient seamen would be available to man additional boats:

“if you went on crowding the ship with boats you would require crew...which would be carried uselessly across the ocean” [8]

Contrary to the statement, there was plenty of crew on board TITANIC but most were engine room and “hotel” workers who were not traditionally required to have maritime skills. Since the designers believed only “seamen” could handle boats, **they effectively only required the number of boats that the available seamen could handle.** They simply could not imagine cross training coal heavers or stewards to handle boats.

CASE 4 ATR -72

The ATR-72 twin engine turboprop passenger aircraft suffered a fatal icing induced crash in 1994 in Roselawn Indiana. Icing had always been a problem for aircraft, due to the weight of the ice. Traditional aircraft design and regulation were based on warning the pilot of icing before the weight of the ice affected the aircraft. These expectations were implicit in the development of the regulatory icing test, which assumed that the effect of icing was linear, gradual and detectable before the aircraft was affected. But engineering innovation in “unpowered” control surfaces and thin wings for turbo props created a new failure mode, sudden “loss of control” due to disruption of the airflow by ice. In the new aircraft, pilots could no longer reliably detect icing before they lost control of the aircraft.

But there was a gap between the innovators and the regulators. Innovators did not address the new failure mode because the wing complied with the existing Federal Aviation Administration (FAA) standards for icing. In the USA the FAA relies heavily on industry in defining and improving safety standards. However, no turbo prop airliners are manufactured in the USA. Instead they are regulated abroad to USA standards. As a result US manufacturers had little interest in the problem of turbo prop airliners. ATR is a Franco-Italian subsidiary of Airbus. The ATR 72 was certified by the French regulator, whose certification was accepted by the FAA. The net effect of this system is that the FAA was regulating in an environment where industry was expected to assist the FAA in identifying flaws in the regulation. But the icing regulation was being enforced by a foreign jurisdiction in accordance with the French technical/regulatory culture in which the manufacturer relies on the regulators to define the technical state of the art. Regulating an innovative technology with a limited regulatory test had produced an entirely new accident path.

Ethics and Regulation

Stating that a product “complies” with a standard thus “begs the question” of the role of ethics in the regulatory process. If the acceptability of the product to the regulator is based on an assurance of safety by an engineer, it is still necessary to define the role of the engineer as advocate for a private party or as steward of the public safety.

Clarifying the role is especially important when engineers are active in influencing the standards or the product acceptance process. Complying with performance standards is a particular problem. Performance requirements do not state how a product is to be made, but grant approval on passing some kind of test or evaluation. Performance requirements normally test certain limited characteristics of a product, and allow regulatory approval if those requirements are satisfied. But what happens when the standards do not cover a relevant characteristic of the product? A product can easily be in compliance with a

performance standard, but contain a hazard not controlled by the standard. As a result, there are at least three interrelated ethical issues in regulatory standards:

- 1) The level of safety actually expected by the standard for each hazard
- 2) The range of hazards actually addressed by the standard
- 3) The role of the engineer in determining both the standard and compliance.

DESIGN PROCESS FAILURE

Our research into the problem of engineering ethics and product design has disclosed a recurring ethical problem that can be described as “design process failure”. A “*design process failure*” is a defective process for producing the design. “Design process failures” do not result in *accidents*. The ensuing disasters are the predictable effects of systems that are designed under processes that disaggregate responsibility for safety. The problem usually arises when no single party accepts responsibility for the overall safety of the design. As noted in the case of the ATR and the TITANIC designers accepted compliance with the code as stating the acceptable level of safety. These appear to be specific instances of the general problem since the same result can occur either deliberately or inadvertently when engineers defer to other engineers or design professionals for a critical aspect of the design. Unless the requirement for the interaction of all components is properly handled, different groups of engineers can, by failure to communicate, create engineered products that fail to “hold paramount” the public safety.

Case 5 Ford Explorer/ Firestone Tire

The Ford Explorer is a Sport Utility Vehicle. (SUV) The Ford Explorer was built on a pickup truck chassis and had a high center of gravity with an enhanced risk of rollover. Tires were designed for the vehicle by Firestone. Tire failure is a leading cause of rollover in SUVs. In pre production tests the Explorer showed an excessive tendency to roll using size 245 tires at 35 PSI. Ford engineers suggested redesign, but management was unwilling to spend the time and money. ““Utilize as many of the chassis revisions as possible without delaying Job 1,” said a Ford memorandum,” [9]

To pass the rollover tests Ford engineers reduced the tire pressure to 26 PSI and used smaller size 235 tires. This reduced the rollover tendency but increased the risk of tire failure. With the smaller tires the payload of the Explorer was only about 800 pounds and tires at low pressure and maximum load tend to fail quite quickly, with catastrophic results. Current litigation is over how and whether Ford coordinated the design change with Firestone. Firestone blamed Ford, Ford blamed Firestone and no one seems

prepared to explain how engineers could have combined to produce such a hazard.

Case 6 The World Trade Center

Leslie Robertson, chief design engineer of the World Trade Center is quoted as saying “ I don't know if we considered the fire damage that [an airplane crash] would cause. Anyway, the architect, not the engineer, is the one who specifies the fire system.”[10]. It is difficult to understand this comment. The fire protection for a structure is part of the engineering design. In the WTC the floors were critical to structural stability yet they were protected to a lower standard than the columns. Was the ball dropped between the professions? Architects have little or no formal training in the complexity of fire protection systems, or the reaction of structural systems to fire stress. Structural engineers typically with *Extrinsic* hazards such as earthquake, wind or rain, and may not fully understand the management problem of *intrinsic* hazards such as the fire load in a building.

Current Problems

Design process failures such as the Kaprun (Austria) ski train fire highlight “design process failure” as a key ethical problem in modern engineering. At Kaprun failures of communication among the civil, electrical and mechanical engineers combined to create an extraordinary hazard that resulted in 155 deaths on a ski train in a tunnel. Kaprun shows that engineers can create hazards faster than society can create regulations to deal with the hazard. [11]

Not only is disaggregation of design responsibility a problem, new methods of engineering design can also create “design process failures” Performance based design can create a conflict of interest when engineers both estimate a hazard and design the performance-based response system. The incentive to minimize the calculated hazard can be overlooked in complex calculations or risk analyses. Regulatory authorities are not responsible for a safe design, but act as a check on the engineer. The ethics of the design process should be judged by the safety of the products designed under that system. Systems have to be developed to make sure that innovations in technology and regulation do not result in compromised public safety. The importance of peer review of engineering judgments can only increase as designs get more complex, less transparent and the consequences of error become more severe.

TEACHING ETHICS

The greatest single problem in teaching engineering ethics is convincing faculty and students that ethics goes beyond teaching personal honesty and integrity. Ethical design requires more than honesty, because a person may honestly believe that a problem is under control when it is not, leading to *design process failure*. Teaching ethical design

means emphasizing the importance of proper system analysis, the impact of conflict of interest, the need for required disclosures of design assumptions, the value of peer review, and compliance with the spirit and intent, not merely the letter of regulation. The key outcome is recognition of the role of ethics in the design process.

CONCLUSION

Law, ethics and engineering are closely related in the design process. Law is inevitably a reactive and blunt instrument Engineering ethics fills a critical gap by making it clear to engineers that they owe a fundamental duty to protect the public. The emphasis in engineering ethics must move from personal integrity to preventing “design process failures”. Protecting the public from the hazards of modern products requires analysis of the many causes of injury and constant vigilance to make sure that engineers really do “**hold paramount**” the public safety

ACKNOWLEDGMENT

This research was supported by the National Science Foundation. Award No. SES-0135945. Ruth Dayhoff MD and Dr Bernd Beier provided assistance on medical ethics. Dr. Beier co-teaches ENES 435. Dr. Fred Mowrer is Co PI on the NSF project and provided assistance on the World Trade Center and performance based design.

REFERENCES

- [1] Burke, J.G. Bursting Boilers and the Federal Power, Technology and Culture, Vol. VII, No. 1, Winter 1966, pp. 1-23.
- [2] LAW FIRMS AND RULE 5.4 PROFESSIONAL INDEPENDENCE OF A LAWYER ABA Model Rules of Professional Conduct
- [3] Case No. 88-6 NSPE Board of Ethical Review
- [4] ASME Constitution, Article C2.1.1.
- [5] Brickman DB and Barnett RL The Grate Debate Triodyne Safety Bulletin available at http://www.triodyne.com/SAFETY~1/B_V4N2.PDF
- [6] Investing in Innovation: Creating a Research and Innovation Policy That Works L. M. Branscomb & J.H. Keller, Editors MIT Press, 1997
- [7] The Regulation of Science and Technology / Edited By Helen Lawton Smith. Houndmills, Basingstoke, Hampshire ; New York : Palgrave, 2002.
- [8] Report on the Loss of the "Titanic." (s.s.) July 30th 1912
- [9] New York Times December 7, 2000, RISKY DECISION/A special report.; Study of Ford Explorer's Design Reveals a Series of Compromises
- [10] Seabrook, J “The Tower Builder” : “Why did the World Trade Center buildings fall down when they did?” New Yorker 11-19- 2001
- [11] http://www.ananova.com/news/story/sm_625271.html?menu=