Chapter 6

RISK AND SAFETY ETHICS

6.1 INTRODUCTION

Risk is associated with engineering in terms of structures, products, processes and materials used in the construction and operation of engineering structures. Invention and innovation introduce an extra element of risk in the lack of knowledge or ignorance about the operational performance of the new products. Examples are the fires caused by damage or overheating that initially occurred upon the introduction of Li-ion electrical batteries into laptop computers, cellular phones, the Volt electric car by General Motors, the Tesla electric car, and the Boeing 787 Dreamliner airplane.

The Li-ion batteries are prized in many advanced products for their high power and long life, but they have been a consistent source of problems across industries. General Motors ended up dropping the Li-ion batteries from its Malibu car hybrids and went back to the lead-acid batteries, finding them cheaper, taking up less space and lowering the risk of battery fire.

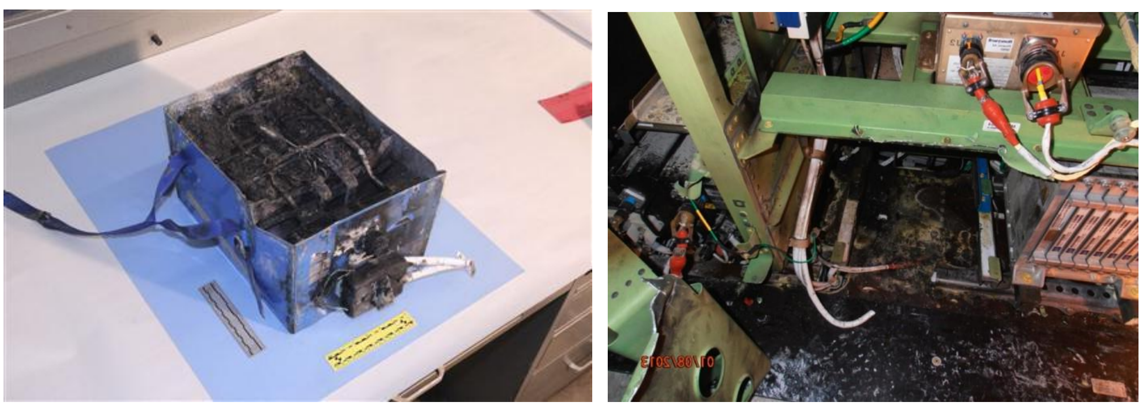

Figure 1. Spontaneously-occurring thermal damage in newly-introduced Li-ion batteries Auxiliary Power Unit (APU) battery in the Boeing 787 Dreamliner Japan Airlines airplane, January 7, 2012 at Logan Airport. Source: National Transportation Safety Board (NTSB).

Figure 2. National Highway Traffic Safety Administration (NHTSA) testing of General Motors side impact safety of the Volt electric vehicle. Source: NTHSA.

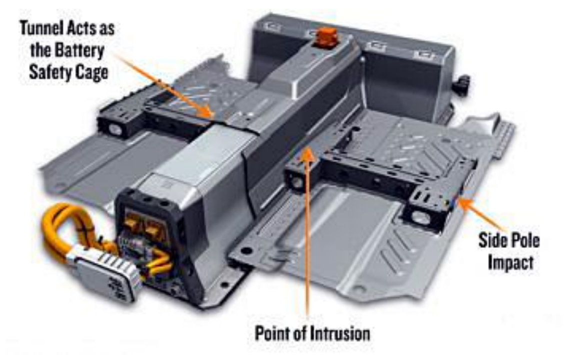

Figure 3. Volt Electric Car battery fix. Source: GM.

Figure 4. Tesla S electric car fire at a highway exit at Kent, Washington. The car hit a "large metallic object" that damaged one of the modules in its liquid-cooled battery pack, which is situated on the underside of the vehicle. The Tesla battery pack is configured as a long, flat slab on the bottom of the car, beneath the passenger compartment and protected by reinforced metal. The case shielding the battery might not have been strong enough to keep the impact from causing a short circuit. Initial attempts to douse the fire were unsuccessful. The fire appeared to be extinguished, then reignited underneath the vehicle. Firefighters had to use a jack to turn the Model S on its side, and then cut a hole in the car to apply water to the burning battery. Possibly unknown to them is that lithium, like sodium is highly reactive with water and air. Source: Video grab.

To ensure a comfortable safety level, engineers are obligated to:

1. Anticipate or predict all the failure modes that can lead to an accident, both at the design and the operational stages.
2. Take into account operational experience and past human and design errors, and incorporate them into their design in view of avoiding catastrophes.

Engineers are also bound by law and by professional ethics to adopt the concepts of "informed consent" towards the public about the involved risks in their designs and projects. The penalty for being uninformed about the laws pertaining to risk, or failing to follow them, could be litigation and damages that could bankrupt the offending individuals or their businesses.

In the USA society and its democratic traditions and institutions, a policy of concealing the discussions from the public is out of the question. It is important to make safety decisions with contributions from the public, considering that the experts themselves could be wrong in their estimates.

6.2 FACTORS OF SAFETY AND IGNORANCE FACTORS

The engineering profession uses the concept of "factors of safety" in its design process. If a structural element will have to carry a maximum load $P_{\max}$, and the design load is P_{design}, the factor of safety FS would be:

$$FS = \frac{P_{design}}{P_{\max}} \qquad (1)$$

For instance, if the maximum load is 1,000 kgs, and the factor of safety is 3, then the design load that must be adopted is 3 x 1,000 = 3,000 kgs.

The accepted engineering practices go further and also introduce "ignorance factors" accounting for the use of untested new materials, configurations, modeling approaches, unpredictable load values, or unaccounted-for emergency uses. For an ignorance factor IF, the design load would be:

$$P'_{design} = IF \, . \, FS \, . \, P_{\max} \qquad (2)$$

As an example, if the ignorance factor is 2, then the design load would be 2 x 3 x 1,000 = 6,000 kgs. A prudent designer will design a structural member that can thus withstand 2 x 3 = 6 times the maximum load. This value of the product of the safety factor and the ignorance factor is the norm rather than the exception in judicious engineering practice.

6.3 REGULATION AND LAWS PERTAINING TO RISK

Numerous laws and regulations pertain to risk. The penalty for being uninformed about them or failing to follow them could be litigation and damages that could bankrupt the offending individual or business.

The 1958 Food, Drug and Cosmetics Act mandates that a chemical “deemed to be unsafe” may not be added to food unless it can be “safely used.”

The concept of “safe use” was defined by the USA Senate Committee on Labor and Public Welfare as meaning that “no harm will result” from its addition to food.

The Delaney Amendment prohibits the addition to food of any chemical known to cause cancer when ingested by animals.

The 1976 Toxic Substances Control Act (TOSCA) asks the Environmental Protection Agency (EPA) to regulate any chemical upon a finding of “unreasonable risk or injury to health or the environment.” TOSCA requires us to take “the availability of substitutes” for substances.

The 1954 Atomic Energy Act refers to the “health and safety of the public.”

The Nuclear Regulatory Commission (NRC) rules use “without undue risk” and suggest a balance between risk and benefits.

6.4 RISK LIABILITY

There is no absolutely-safe technology with risk totally eliminated. Accidents do occur and can lead to legal action for damages in the case of products failures or design flaws.

For instance, the threat of being subjected to liability legal action in the form of malpractice law suits has been an issue for physicians as well as engineers, accountants, lawyers and other professionals.

LAW OF TORTS

The litigation seeking redress from harm most commonly appeals to the law of torts. This law deals with injuries to a person caused by another, usually as a result of negligence or fault of the injuring person.

An example is the litigation from harm resulting from asbestos exposure against Fiberboard Paper Products Corporation due to the irreversible lung disease known as pulmonary asbestosis causing the mesothelioma lung cancer. Another example involved the exposure to Poly-Chlorinated Biphenyls (PCBs) causing cancer, against the Witco Chemical Corporation and the Monsanto Company. Other cases involved exposure to the paraquat and to the Agent Orange herbicides.

In tort law, the standard of evidence is the “preponderance of evidence.” This means that there is more and better evidence in favor of the plaintiff than the defendant. It is a lower standard of evidence and is less stringent than criminal proceedings which call for proof “beyond reasonable doubt,” and those demanded by the standards of proof in science requiring for 95 certainties or confidence levels.

6.5 PROFESSIONAL ETHICAL AND PROFESSIONAL CONDUCT CODES

Safety is given a prominent place in all the engineering professional codes. Engineers are expected to uphold the safety, health and welfare of the public. The statements in the codes concerning safety are related to the concept of risk.

The American codes use the term “safety” but rarely the term “risk” even though they are closely associated. However, the London Institute of Mechanical Engineers (IMechE) Joint Code of professional Practice and Risk Issues is a ten-points code that discusses professional responsibility, the law, and professional conduct regarding risk.

NATIONAL SOCIETY OF PROFESSIONAL ENGINEERS (NSPE)

The National Society of Professional Engineers (NSPE) Code of Ethics for Engineers first canon requires engineers to: “Hold paramount the safety, health and welfare of the public in the performance of their professional duties.”

It requires engineers to design safely in terms of “Accepted Engineering Standards.” It encourages engineers not to “Complete, sign 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.”

Concerning informed consent, it instructs engineers that if their professional judgment is overruled in “Circumstances where the safety, health, property or welfare of the public are endangered,” they are obligated to “Notify their employer or client and such other authority as may be appropriate.”

The Accreditation Board for Engineering and Technology (ABET), formerly the Engineer’s Council for Professional Development (ECPD) has the following professional ethics code:

CODE OF ETHICS OF ENGINEERS (ABET)

The Fundamental Principles

Engineers uphold and advance the integrity, honor and dignity of the engineering profession by:

I. Using their knowledge and skill for the enhancement of human welfare;
II. Being honest and impartial, and serving with fidelity the public, their employers and clients;
III. Striving to increase the competence and prestige of the engineering profession; and

IV. Supporting the professional and technical societies of their disciplines.

The Fundamental Canons

1. Engineers shall hold paramount the safety, health and welfare of the public in the performance of their professional duties.
2. Engineers shall perform services only in the areas of their competence.
3. Engineers shall issue public statements only in an objective and truthful manner.
4. Engineers shall act in professional matters for each employer or client as faithful agents or trustees, and shall avoid conflicts of interest.
5. Engineers shall build their professional reputation on the merit of their services and shall not compete unfairly with others.
6. Engineers shall act in such a manner as to uphold and enhance the honor, integrity and dignity of the profession.
7. Engineers shall continue their professional development throughout their careers and shall provide opportunities for the professional development of those engineers under their supervision.

Different professional societies have also their own codes of ethics. The Institute of Electrical and Electronics Engineers (IEEE) has the following ethics code:

CODE OF ETHICS (IEEE)

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. To accept responsibility in making engineering decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. To avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. To be honest and realistic in stating claims or estimates based on available data;
4. To reject bribery in all its forms;
5. To improve the understanding of technology, its appropriate application, and potential consequences;
6. To maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. To seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contribution of others;
8. To treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;

9. To avoid injuring others, their property, reputation, or employment by false or malicious action;
10. To assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

6.6 RISK PERCEPTION

The usual definition of risk is the product of likelihood of an adverse effect p_i and its consequence or the magnitude of the adverse effect or harm C_i :

$$R_i = p_i C_i \tag{3}$$

The overall technological risk is thus a summation over all the n different modes of occurrences of failures:

$$R = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} p_i C_i \tag{4}$$

For most people the perception of risk involves other factors that are value judgments including:

1. The equity of risk,
2. The control of risk,
3. The understanding of risk.

Equity refers to justice or fairness in the distribution of risk and who gets the benefits from it among those who share it.

Controlling the hazard considers whether the hazard is voluntarily assumed. Those voluntary risks such as smoking are readily more acceptable than those imposed by building an industrial polluting facility in one's neighborhood.

A risk that is understood through informed consent is evaluated in a different way than one that is poorly explained.

6.7 RISK ASSESSMENT METHODLOGIES

Risk assessment is considered as an uncertain prediction or anticipation of the degree of harm. It is estimated by several established methodologies.

1. Fault Tree Analysis:

Fault Tree Analysis is used to anticipate hazards to which there is little prior experience. The different failure modes of the components of a system are combined to infer the behavior of the overall system. The algebra of Boolean Logic and Probability Theory are used as an exact mathematical way to describe the inherent uncertainty in a system in the form of randomness. Alternatively, Fuzzy logic and Possibility Theory are another exact mathematical way to describe another form of uncertainty in the meanings or the fuzziness in the words we use to describe different hazards. An even more powerful methodology involves the coupling of Probability Theory to Possibility Theory. In Fault Tree analysis deductive reasoning or backward-chaining is used in the application of the algebra of logic.

2. Event Tree analysis:

Event Tree Analysis is an inductive logical reasoning or forward-chaining process is used instead, with the postulation of an initiating event that is followed through the system as to its logical consequences and their associated probabilities and possibilities.

6.8 LIMITATIONS OF EXISTING METHODOLOGIES

Whereas Probability Theory and Possibility Theory are exact methodologies that quantify the uncertainties involved in random measurements and fuzzy modeling of nature, they themselves possess their own uncertainties.

The successful application of these methodologies must recognize their usefulness as well as their limitations:

1. One cannot claim to be able to fully anticipate all the mechanical, physical, electrical or chemical initiating events that can lead to the failure of the components of a complex system.
2. The possible human errors that can lead to failure cannot all be anticipated.
3. The models used to estimate the failure probabilities or possibilities are subsets of the actual system. They consider the most important parameters that are thought to govern the system. If an important parameter is missed in the modeling, a mismatch between the actual system and its model would occur leading to instability.
4. Design or operational flaws may have crept into the design of the system or into its operational mode, but are not considered in the modeling process.

Despite the existing limitations, responsible engineers must try to anticipate at the design stage of an engineering system the probable and possible failure modes. Once operational, the system must now be monitored and controlled in such a way that the performance levels of the individual components and its subsystems are continually estimated so as to anticipate any future malfunction. The system should thus be steered away from the undesirable future state to a favorable one. Just reacting to the occurring malfunction should be replaced by predicting and avoiding its occurrence altogether.

6.9 RISK BENEFIT OR COST BENEFIT ANALYSIS

The concept of “utilitarianism” suggests that the answer to a moral question is the particular course of action that would maximize human, and some extend it to the overall environment, well being.

Adherents to the utilitarian concept accept the economical technique of cost benefit analysis also called marginal cost analysis as a useful tool in assessing risk.

In its application to the estimation of risk it is also referred to as “Risk Benefit Analysis.” The justification for the terminology is that the cost is usually measured in terms of deaths, injuries or other harms, as much as it could be expressed in terms of monetary figures. Either terminology is commonly used.

Cost benefit analysis possesses the same limitations of utilitarianism:

1. It may not be possible to anticipate all the costs and benefits associated with different design options, leading to an inconclusive result.
2. It may not always be possible to translate the risks and benefits into monetary or dollar terms.
3. Allowance for the distributions of costs and benefits may not be possible. A majority of the population may benefit at the expense of a smaller minority that would suffer.

In spite of these limitations cost benefit analysis has a recognized and legitimate place in risk assessment. It excels when no serious threats to individual rights are involved. It is a systematic and objective approach providing a meaningful way of comparing risks, benefits and costs using a common measure of dollars and cents.

6.10 RISK VALUES AND ORIENTATIONS

The concept of acceptable risk defines the professional and ethical dimension of the engineering profession. Because of the element of uncertainty involved in risk, a bias or predisposition in favor of one set of values or another is inevitable. Two sets of values, biases or orientations can be identified:

1. The Good Science (GS) approach

In this approach one avoids the prediction of hazards to public health and safety where none do in fact exist. The burden of proof of the existence of a postulated risk is on those who claim that such a risk could exist. It protects the rights of producers of new technology and avoids burdening them with excessive regulations. This approach evidently promotes innovation and economic growth.

2. The Respect for Persons (RP) approach

In this restrictive approach, one attempts to discover as many threats to public health and safety as possible and incorporate them in the design process. The burden of proof is shifted to those who claim that the risk from a new technology is acceptable. The approach claims to protect the public from risks even at the expense of economical efficiency. This means that the interests of the individual users of a given technology are favored compared with the rights of the developers of the technology.

According to this ethical perspective, it is wrong to deny the moral agency of individuals. Moral agents are defined as beings capable of formulating and pursuing purposes of their own. Moral agency is protected by rights to life, health, physical integrity, not to be deceived; as well as the right to free and informed consent to risks that could infringe on these or other rights.

This form of ethics places the greatest emphasis on the rights of individuals, irrespective of the costs to the larger society.

6.11 PRINCIPLE OF ACCEPTABLE RISK

Because of the conflict between the utilitarian and respect for person approaches to risk, the two concepts need to be combined. The respect for persons component must emphasize informed consent and individual rights and the protection of individuals from harm. The utilitarian approach must consider the consequences to the general welfare to society from the regulation of risk. It must balance the protection of the individual against the need to protect technologies that are irreplaceable and result in great benefits to society. From that perspective it is unimaginable that regulations can be issued to eliminate cars even though they cause about 50,000 deaths / year in the USA.

A principle of acceptable risk is proposed by Harris, Pritchard and Robins [1] that provides guidance in determining when risk is within the bounds of moral permissibility:

> "People should be protected from the harmful effects of technology, especially when the harms are not consented to or when they are unjustly distributed, except that this protection must sometimes be balanced against:
> a) The need to preserve great and irreplaceable benefits, and,
> b) The limitations on our ability to obtain informed consent."

They warn that the proposed principle does not offer an algorithm to be applied mechanically to situations involving risk. Its application must consider the particular situations, each according to its own merit. For instance, implementation of the requirement to reduce risk in the coal industry should not lead to the destruction of the coal industry.

They point out that the engineering profession's responsibility to protect the health and safety of the public requires it to reduce risk when this can be done as a result of the available technology.

6.12 DOCTRINE OF INFORMED CONSENT

The engineering profession has the responsibility to promote conditions under which individuals are able to give informed consent to risks they are exposed to as a result of exposure to a given technology, particularly when these risks are unusual in their nature.

A disparity exists between the expert's and members of the public perception of risk in that the public perception involves various value judgments:

1. **Anchoring effect**:

Behavioral psychologists study a phenomenon called "anchoring." People tend to take recent events and project them into the future in a straight line. We "anchor" our projections on some number or data we have recently seen. Tomorrow will be like today.

The public is usually mistaken in estimating the probabilities of injury or death from different activities or technologies. Chauncey Starr [2] has noted that: "laypeople tend to overestimate the likelihood of low probability risks and to underestimate the likelihood of high probability risks associated with causes of death." This leads to "anchoring" or overconfident biasing. In this case an original estimate of risk is made; an estimate which may be quite erroneous. Even though new estimates are generated, the original estimate "anchors" future estimates and precludes adjustments in the face of new evidence.

Experts consistently are an order of magnitude low (10 times) in their perceptions of the perceived risk. Members of the public, on the other hand, are even more mistaken than experts in that they are two orders of magnitude lower (100 times) in their perception of risk.

2. **Voluntary versus involuntary risk effect**:

According to Chauncey Starr, members of the public are willing to assume some voluntary risks, such as smoking, that are three orders of magnitude (1,000 times) as uncertain as involuntary risks, such as a waste dump construction next to one's house. Members of the public think of an involuntary assumed risk as inherently more risky than one that is voluntarily assumed, with an involuntary risk perceived as 100 times that of a voluntary assumed one.

3. **Compensation effect**:

The level of risk R people are willing to accept in the workplace is proportional to the cube of the increase in the wages W offered for the additional risk:

$$R \ \alpha_{\ell} \ W^3 \tag{5}$$

For instance, doubling the wage to 2W, convinces a worker to accept $2^3 = 8$ times the original level of risk.

4. **Human versus natural origin**:

If the risk has a human origin, the perceived risk is 20 times as large as the perceived risk having a natural origin.

5. **Timeliness**:

An immediate risk is perceived as being 30 times larger than a delayed risk.

6. **Catastrophic versus regular risk**:

A catastrophic risk is perceived as being 30 times larger than an ordinary one.

7. **Regular versus occasional risk**:

A regular risk is perceived by the public as being just as large as an occasional one.

8. **Necessary versus luxury risk**:

A necessary risk is also perceived by the public to be just as large as a luxury risk.

6.13 PRECAUTIONARY PRINCIPLE

In most of Europe, the precautionary principle is adopted. It suggests that when there is enough data to have a suspicion of harm, one can go ahead and act without having to have absolute proof of harm.

This places the burden of proof more on people who for instance market pesticides to show that the claim of no harm is unfounded. In the USA, to ban a pesticide one has to show proof of harm.

According to this principle in France, Italy, Germany and Slovenia, a class of pesticides known as “neonicotinoids” in the market since the 1990s and widely used for the treatment of seeds on 120 agricultural crops was banned after they were suspected of finding their way into the pollen and impair honey bees navigational and foraging abilities causing the “Colony Collapse Disorder” or CCD syndrome. The observation is that bees lose their orientation capabilities and cannot navigate their way back to their hives causing its depopulation and demise.

6.14 DISCUSSION

The different perceptions lead to different federal and state governments programs to reduce risk spending ranging from $170,000 to $3 million per life saved, under public pressure.

The fact that the public estimates risks differently from experts poses a serious ethical issue. In a society with democratic institutions, a policy of concealing the discussions from the public is out of question. It is important to make safety decisions with contributions from the public, considering that the experts themselves could be wrong in their estimates.

The ideal solution is to educate the public to see the problem of risk estimation the way that the experts do. This approach fails due to the fact that the public will always include value judgments.

The only viable alternative is a combination of expert and public approaches that include:

1. Free and informed consent by those subjected to risk.
2. A fair distribution of the risks as well as the benefits.
3. The adoption of a democratic process of decision making.

Members of the engineering community would have to adopt projects that inform the public about risk and to encourage engineers who possess the most reliable information about risk to fully participate in these projects. This involves the following considerations [1]:

1. Awareness of the uncertainties as well as the value dimensions of the different phases of the analysis and treatment of risk.
2. Awareness of the limitations of Cost Effectiveness Analysis regarding the added need for the fair distribution of risks and benefits.
3. The promotion of democratic and free informed consent and democratic decision-making in matters of risk exposure.
4. Develop their abilities to think competently and clearly about the ethical aspects of risk.

EXERCISES

1. List three factors that govern the perception of risk in most individuals.

2. The concept of acceptable risk defines the professional and ethical dimension of the engineering profession. Because of the element of uncertainty involved in risk, a bias or predisposition in favor of one set of values or another is inevitable. Explain the difference between the observed two sets of values, biases or orientations:
i. The Good Science (GS) approach
ii. The Respect for Persons (RP) approach

3. Describe by an example how the "Precautionary Principle" is applied in Europe and in the USA.

4. For a maximum load of 500 kgs on a structural element, what is the design load for a factor of safety of 3 and an ignorance factor of 2?

REFERENCES

1. Charles E. Harris, Jr., Michael S. Pritchard and Michael J. Rabins, "Engineering Ethics: Concepts and Cases," Wadsworth Publishing Company, 1995.
2. Philip L. Alger, N. A. Christensen, and S. P. Olmstead, "Ethical Problems in Engineering," New York, Wiley, 1965.
3. M. D. Bayles, "Professional Ethics," 2nd edition, Belmont, California: Wadsworth, 1989.
4. D. Callahan and S. Bok, "Ethics Teaching in Higher Education," New York: Plenum Press, 1980.