Educating – risk

Ron B. Ward

University of New South Wales
Sydney, Australia

ABSTRACT: This paper follows from a previous one, which looked at the problem of educating engineering students, particularly undergraduates, in aspects of industrial safety; this paper goes the next step in a conceived sequence by considering what engineering students, again specifically undergraduates, need to know about risk. After defining risk, and considering some of what has been written on the topic through the last few decades, we come to the application of probability on risk-thinking, how it may be relevant and how probability can be misapplied, particularly in the connection between risk and engineering. From that the concept of residual risk is reached, what is left over after all precautions have been taken, the remainder with which people must live, and the ultimate source of mistakes, mishaps and disasters of all magnitudes. Where does this impact on the undergraduate engineering student? By generating awareness that things can go wrong and accept that engineers must examine all aspects of a problem in a design or of an operating system, using imagination as well as rational thinking, rather than trust the calculations.

INTRODUCTION

What is this we refer to as *risk*? It is used in our language so often these days, yet one seldom gets a clear indication of what it means in a particular context. It should be noted that the author discussed risk in detail in his Doctorate thesis and much of the following is taken, with some modification and addition, from that [1].

That lack of clarity may be because the concept of *risk* can be presented in many different ways. Risk may be *forecast*, *identified* and *assessed*. A situation may cause those present to be *exposed* to risk. Risk may be *measured*, *evaluated* and *avoided* or *accepted*. After that, risk may be *controlled*, *mitigated* or *transferred*. Finally, there can be risk *consummation* and *litigation*, after which only the lawyers win.

An important point is that there is nothing new in all the above; the concept of risk and how to deal with it, particularly in engineering, has been around for a long time as evidenced by the dates on many of the references cited.

SOME QUALITATIVE DEFINITIONS

Risk can be presented in many different ways, and some of them are explored below.

The English word *risk* is apparently derived from the French *risque*, which translates simply as *risk* [2]. But *risque* has rather unfortunately been retained in English with a different meaning: *of doubtful propriety, suggestion of indecency*, even though it is unchanged in the original language [3]. A quick search through the indexes in the back of a dozen books on the author's shelf discovered no definitions. Then two were found.

Mondarres simply defined risk as: *The potential of loss or injury resulting from exposure to a hazard* [4].

However, that requires a definition of the term *hazard*. For example, the following statement is given:

> *A condition or situation which has the potential to create or increase harm to people, property, or the environment.* A set of conditions in the operation of a product or system for initiating an accident sequence (from BS4779:1979) [5].

Viner quoted Rowe, who gave a very brief definition of risk: *The potential for the realisation of unwanted, negative consequences of an event* [6].

Two other books with *risk* in the title had the word in the index; one discussed it in terms of directors' duties, the other in terms of perception, but neither approached the succinctness of the two above.

So what do engineering organisations have to say about risk? A very elementary definition of risk was given by the Institution of Engineers, New Zealand (IPENZ): *The combined effect of the probability of occurrence of an undesired event, and the magnitude of the event* (from BS4779:1979) [5].

An interesting reflection on that came from Steele, who used the word *consequence* instead of *magnitude*, and pointed out that the *cost* of avoiding the consequence could be considered instead of the *consequence* itself [7].

A general definition, similar to that from the IPENZ but which concentrated on the probability aspect of risk, was given by the UK Institution of Chemical Engineers (IChemE):

> *The likelihood of a specified undesired event occurring within a specified period or in specified circumstances. It may be either a* ***frequency*** *(the number of specified events occurring in unit time) or*

> *a **probability** (the probability of a specified event following a prior event), depending on the circumstances* [8].

The bold emphases are in the original.

A broader definition combining many aspects of risk has been quoted by the USA Center for Chemical Process Safety as follows:

> ***Risk*** *is a combination of* ***uncertainty*** *and* ***damage****.*
> ***Risk*** *is a ratio of* ***hazards*** *to* ***safeguards****.*
> ***Risk*** *is a triplet combination of* ***event****,* ***probability****, and* ***consequences*** [9].

Again, the emphases are in the original.

The above shows the concept of *risk* contains many elements that combine in many ways. So, summing up all the above, it can be concluded that risk comprises the following:

> *The possibility of the occurrence of an uncertain event, resulting from the existence of a hazard, which event may be specified in terms of its probability or its frequency of occurring after a prior event and the magnitude or severity of the consequence.*

These definitions demonstrate the complexity of the topic. Their including the terms *frequency* and *probability* introduce the mathematical or quantitative concept of risk.

The term *consequence* has already appeared above, and will reappear many times below. From and engineer's viewpoint risk can have many possible consequences, for example:

- Loss of assets;
- Loss of use of assets;
- Personnel injuries;
- Public liability;
- Environmental damage;
- Legal consequences – duty of care and negligence:
    - Third party claims;
    - Contractual claims;
    - Professional indemnity.

SOME QUANTITATIVE DEFINITIONS

Quantifying risk with any satisfaction is difficult because the perception level varies from one observer to another. The *actuarial* response is the use of mathematics to define, analyse and present risk. However, the technically-oriented writers have defined risk in a quasi-mathematical manner, in line with the IChemE definition, that risk is a function of two interlocked variables as follows:

$$\text{Risk} = f\,(\text{Frequency \{or probability\}} \times \text{consequence})$$

The precise interaction between those variables is far from precise, hence the use of the *function* type of equation.

The term *consequence* is on a time basis, for example annually, by relating it to events occurring in the same period:

$$\begin{array}{c}\text{Consequence}\\\text{per unit time}\end{array} = \begin{array}{c}\text{Events}\\\text{per unit time}\end{array} \times \begin{array}{c}\text{Consequence}\\\text{per event}\end{array}$$

This can be illustrated by this numerical example, which assumes a hypothetical facility will have an explosive disaster once in 550 years, based on historical records of similar systems, which records also indicate one person in 100 present has been killed in such an event [10]:

$$\begin{array}{c}\text{Likelihood of}\\\text{deaths per year}\end{array} = \begin{array}{c}\text{1 explosion}\\\text{per 550 years}\end{array} \times \begin{array}{c}\text{0.01 deaths}\\\text{per explosion}\end{array}$$

$$= 18.2 \times 10^{-6} \text{ deaths per year}$$

$$= \text{approx 20 per million, or 1 per 50,000 years.}$$

One great difficulty with such a calculation is that no tolerance or margin is given or implied to the 550 years, so, is it precisely that? Or is it plus or minus 10%? If the answer is, as in the above example, one death per 50,000 years, then which year? In 500 years? Or 10 years? Or next year? This year?

The same question applies to the one-person-in-100 being killed. Who will it be? The person nearest to what happens? These figures are both from observations, but are the figures affected by recent larger or smaller variations? And what population was involved? One should question the one-in-100 death, was it only *one*, or was it two in 200, three in 300, and so on?

Unlike the above equation, some single disasters have caused a relatively large number of fatalities. Kletz looked at several possible ways of valuing a life, including the cost of saving a life. He raised and discussed several objections, then considered the problem of multiple casualties as follows:

> *When a number of people are killed at a time the public outcry is greater. People are prepared to spend more to prevent these multiple casualties. Should the value ascribed to life increase as the number of people killed at a time increases?*
>
> *There is no real difference between an industry that kills 100 people one at a time over a 10 year period and one that kills 100 at a time every ten years.*
>
> *Perhaps also society is not entirely wrong in preferring 100 single deaths to 100 deaths at a time – the latter disrupts a whole community, mentally and physically, and the wounds take longer to heal* [11].

The equation looks satisfying as a mathematical statement, but the result is as hard to interpret precisely as answers from the Oracle of Delphi.

THE MANY FACES OF RISK

Individual risk is the risk to one person. Using the word *person* in a legal sense would include a *corporation*, a business entity. This has been defined by IChemE: *Individual risk – the frequency at which an individual may be expected to sustain a given level of harm from the realisation of specified hazards* [8].

Instead of for one individual person, risk may be expressed for a population, ie as societal risk: *The concept of societal risk provides a measure of the chances of a number of people being affected by a single event or a set of events* [12].

IChemE has covered that in a similar manner:

> *Societal risk – the relationship between frequency and the number of people suffering from a specific level of harm in a given population from the realisation of specified hazards* [8].

These definitions only provide *a number of people* and *how often*. All risk statements are similar in this respect, including the general definitions above. They do not state specifically *which person* and *when*.

Another general definition of risk (given by Kuhlmann) states how risk applies to business situations as follows:

> *Individual and global risk. From a linguistic point of view, the concept of* risk *has practically the same connotation as* venture *or* hazard*. In the economic environment, however, it includes the possibility of loss as well as the expectation of gain.*
>
> *Consequently it will be safe to regard* risk *– in its more general usage within the terminology of safety science – as a* certain level of danger *relating to a group of possibly affected people and to a period of time in the course of which such a loss or damage constitutes a distinct possibility* [13].

The Institution of Engineers, Australia (IEAust), has expressed concern about the risk exposure of professional engineers in their work situations. This is a form of business risk, in the professional occupation, as well as personal risk to the individual engineer in practice. At present, professional engineers can only protect themselves by professional indemnity insurance.

In the paper examining the situation current in November 1990, IEAust expressed the hope that existing laws would be changed and new laws enacted to protect the professional engineer who applies reasonable judgement from prosecution for negligence [14]. A follow-up paper from the same organisation expressed the same ideas, but focused on areas more closely linked to this present study than the more general statements of the earlier paper. The areas of special interest were as follows:

- The issues that are important to engineers;
- The social construction of risk;
- The engineering construction of risk;
- The human-technology interface;
- The management of expectations [15].

The paper concluded with a 10-point code of good practice for dealing with these specific areas of risk [15].

PROBABILITY

Probability has been mentioned in the above discussion in the mathematical definition of *risk*, used in the definitions of *risk*, and is the *chance* or *likelihood* of the particular event occurring. Some of the preconceptions attached to the term *probability* in everyday language unfortunately cloud understanding so that many people seem to have the general impression that probability is entirely subjective.

However, probability can be defined objectively. Texts on probability (eg ref. [16]) quote the three *postulates of probability*, which state in axiom form certain agreed limitations on how the concept is used such as the probability of a certain event occurring is based on the frequency of that event through a large number of observations. If, say, one thousand observations are made and the identified event occurs 50 times, the probability of it occurring in the future is said to be 5%. Thus, probability can be expressed in terms of *frequency of occurrence*, as follows:

> ***Definition:*** *If an experiment e gives rise to a sample space having a finite number, n, of equally likely outcomes, then the probability of the outcome of any event, say event A, is the ratio of the number of outcomes contained in A to the total number of outcomes* [16].

The further difficulty in applying classical probability reasoning to the study of risk is the inclusion of the term *equally likely outcomes* in the above definition.

CREDIBILITY VERSUS PROBABILITY

Having objected above to expressing probability subjectively, one must now admit that there is a subjective aspect. Perhaps, rather than say this is subjective, it should be classed as *judgementive*, which is how credibility influences probability.

A decision-maker must judge a possible event to be a credible risk before progressing to accepting (or otherwise stating) the probability of the event occurring. Just as impossible events have zero probability, events of very low probability are non-credible. In the range of *possible events*, some will be outside the *credibility range* of those who are experts in the particular field of study, and these experts will insist on considering only *credible events* as those which have a real probability of occurring [17]. However, the risk may be well within the credibility range of those members of the general population who may regard *any* possible event as credible.

A simple illustration of the above comes from the relationship between the three sides of what is known as the fire triangle: flammable material, oxygen and a source of ignition. Consider an open container in the shape of a dish so that liquid on it has a large area exposed relative to its volume or mass. Now consider a quantity of acetone is poured into the container and the dish is left open to air. Acetone has a very low flash point of -18° C (the temperature at which the vapour will ignite in air, given a source of ignition) and is, therefore, very easy to ignite. There now is a highly flammable material and oxygen, and the question which follows is: can a fire be expected? The answer is, obviously, *no*, because there is no source of ignition. However, the *probability* of a fire may be discussed, based on the *possibility* (or probability) of a source of ignition approaching the container, and to reduce that possibility (and the related probability) many types of protection may be introduced, either hardware or software, or both.

Now suppose the acetone is stored in a secure that has appropriate hardware in the form of flame-trapped vents and monitoring equipment, has a nitrogen gas blanket supplied to exclude oxygen, and has all sources of ignition many metres distant. The *probability* of fire is now reduced to a very low level and, in such a case, the technical expert will state that a fire is non-credible, even though still *possible*.

Taking the situation a little further, if the tank is also fitted with appropriate alarms to alert personnel to the imminence of a fire conditions and also with a foam extinguisher system, it may be concluded that a fire is still *possible*, but the *probability* of the fire actually happening is quite non-credible.

Whether such a shift of probability from high to low, comparatively, is acceptable raises the question of *risk acceptance*.

RISK ACCEPTANCE

The definition of risk acceptance is quoted by IPENZ from *The Acceptability of Risk* by the Council for Science and Society: *Acceptance of risk refers to responsibility. A risk may be accepted in ignorance, or inadvertently, or intentionally* [6]. This definition shows that risk acceptance may occur through knowledge of the risk (the converse of ignorance), or through lack of knowledge (that is, ignorance). *Knowledge* suggests that the person accepting the risk would feel *safe* with that knowledge: *A thing is provisionally categorised as safe if its risks are deemed known and in the light of that knowledge judged to be acceptable* [6].

The question arising from that is: how may an individual judge whether a risk is acceptable? The growth of technology through last Century provides a relevant example: is the risk of using a new item of technology *acceptable*? A review of the problem has produced a series of *technology perception hypotheses*, which suggest inter alia that *sub-groups* (eg experts, advocates, students) define risks differently [18]. Slovic summed up that problem as follows:

> *Whereas technologically sophisticated analysts employ risk assessment to evaluate hazards, the majority of citizens rely on intuitive risk judgements, typically called* risk perceptions [17].

When a *new risk*, for example, from a technological innovation, is to be introduced, the person who will experience the risk should be allowed to know what the risk is, *then* the individual can compare the new risk with others *which have been accepted in the past. An acceptable risk is one that does not cause an individual or society to change the level of that risk* [6].

The two principal divisions into which *an individual* may fall are those who know the risks around them and those who do not. The above illustrates a point made by many writers (eg Slovic et al [19]) that acceptance of risk may be *voluntary*, in which case the individual knowingly accepts the risk, or *involuntary*, where those accepting effectively have the risk thrust upon them.

As an illustration of this distinction, operators in chemical and nuclear power plants today are almost certainly in the first category: accepting risk voluntarily. They know the risk situation exists and they accept it. In parallel, they accept an income. The dual acceptance of risk and income is based on an intuitive cost-benefit decision. Contrawise, people living near a chemical or nuclear power plant may, or may not, know there is a risk. Whether they have any knowledge that the plant exists, or whatever level of risk is present, or not, they accept the risk of proximity to the plant involuntarily.

Risk is related to probability, which should be based on data and objective reasoning. Risk acceptance, voluntary, by individuals and organisations, depends on knowledge, data, and hence objective reasoning. Risk acceptance, involuntary, by individuals and organisations occurs with the lack of knowledge and data, and may therefore be based on subjective reasoning.

There is another aspect of risk acceptance, a failure to accept or an avoiding of acceptance. The classic example comes from the attitude of people living downstream from a large dam; they clam up mentally about the possibility of the dam bursting and flooding where they live. This goes through four stages:

1. Failure to anticipate a problem, which is thinking about what might eventuate;
2. Failure to see a potential problem that exists;
3. Failure to try to solve the problem;
4. Failure to solve the problem.

The term *psychological denial* has been applied to this situation.

As remarked above, insurance may be taken out to cover risk, a business action that is not accepting risk but off-loading it by making it someone else's problem.

Much of the above, although with a more societal slant (and somewhat anti-technology) was covered by one of the first to write on acceptability, Lowrance [20].

Now to the type of risk engineers of which must be aware.

TECHNOLOGICAL RISK

This aspect of risk, associated with any aspect of technology, is usually related to the efforts of engineering people to harness the forces of nature, even in a way that seems rudimentary to this Century's thinking. This is not new: Fremlin gave a figure for the possible number of drownings in millponds in the century when water was the main source of power for machinery, which shows fatalities from technological risk were occurring and were recognised centuries ago [21].

Taking one industry as an example, technological risk is a necessary consideration when one considers the combination of materials, processes and engineering in the chemical industry, particularly the petroleum sector. It is been remarked, rather wryly, that by now there are enough oil refineries in the world for one to be blazing merrily every day of the year; perhaps that an industrial version of *urban myth*, but it illustrates the risk of dealing with flammable liquids, explosive gases and toxicity in a work environment involving high pressures and temperatures, and literally open flames in furnaces. Living comfortably in such conditions is only possible, indeed credible, by use of controls such as those mentioned above in the section headed *Credibility versus Probability*.

Steele linked technological risk, particularly innovative technology, with business risk and societal risk, and to some extent with individual risk:

> *Risk can be thought of as resulting from movement away from the existing state of affairs of any of three dimensions: technology, product, and market, with the first being separated into product and process, and the last being subdivided into customers and channels of distribution* [7].

The above indicates that innovation, that is, change, involves risk. Confronting and dealing with the risk in new and innovative technology has been considered by several writers. The general consensus appears to be that the distribution of accepting risk-taking with new technology is unevenly distributed in that *experts* find it easy, but *laypersons* find difficulty [19].

AN INTERESTING REFERENCE

Many of the references cited above go back years into the past; they have been used to show that the concept has been discussed for quite a long time. One is now mentioned that is reasonably recent and which is worth reading for reasons other than for application to engineers' thinking processes [22].

The book by Adams is worth reading because, first, it covers the Royal Society's 1983 report on Risk Assessment, with the distinction between objective risk (what the experts see) and perceived risk (what is evident to the man and woman in the street). It covers much of the uncontrollable risk we meet day by day, weather, climate, traffic and so on, with some diagrams illustrating applications of risk [22].

However, many of those features make it unappealing to the author as an engineer, because we (engineers) deal with external risks that we cannot control (like weather) so we accept, live and work around them, and professional risks we can control (such as selection of materials and correct design).

EXPERT VERSUS LAYPERSON

The different viewpoints between those groups has been mentioned twice above, so now to an observation of their coming together.

Several decades ago, the author worked on an LPG terminal proposed for a location not far from the airport, where several similar conditions-of-risk were already present. There was no objection from the airport management, or from the other sites already occupied, but a large number of local people arrived at the public meeting with strenuous objections to the proposal. One was a keen angler who was concerned about the possibly reduced catch in Botany Bay. A woman put up an objection with no background reason; she merely objected. Another worried about a 747 landing on the site and igniting over a thousand tonnes of LPG (although the location was off the flight path). And so on. But the experience demonstrated that Mr and Ms J. Public see technology in a light different from that which illuminates a project for an engineer.

RISK MANAGEMENT

This is the aspect of risk which has been given much attention in recent years, and has been covered very well (that is, as far as possible) by AS4360 [23]. This is a very common-sense review of the subject and its application. After preliminary chapters on definitions and requirements, it moves to the management process, which covers identifying, analysing, evaluating, accepting (yes or no?) and treating risks.

Only two reservations can be suggested in the use of this document. One is that there seems to be no indication that the process depends very heavily on having people with good imagination and who will believe *things can go wrong*. This opinion came from the author's memory of a design team on an LPG project in which one member refused to accept that something could go wrong with his instrumentation, which was designed to be *foolproof and failsafe*. He was overruled by a majority who agreed people could not be prevented from making mistakes (foolishly or otherwise) and external factors like power failures occur.

The other reservation is the standard gives the impression risks can, actually, be *managed*, which is true, but only up to the point where the potential becomes reality, hence going through the steps recommended may introduce a level of complacency leading to apathy. That, in turn, can lead to crisis, which is (as Kipling wrote on several occasions) another story.

Aside from those reservations, purely personal by this author, AS4360 is a better treatment of risk management than many of the texts reviewed, is an excellent coverage of a difficult matter and is worth using.

There are many references on risk management. The author cites here only Ardis and Comer, as well as and Kendall, both of which are on business risk and management, and Wang and Roush, which is on engineering risk (Mondarres, also on engineering risk, was cited earlier) [4][24-26]. But the idea of risk management was covered long before those [27].

There may be something missing from the risk management portfolio: there is a good consideration of many aspects within a possible project (for example), but not how to deal with managing the risk perceived by those laypeople. They see problems not visible to the expert, and require a form of management closer to public relations.

A SIMPLE EXAMPLE OF RISK AND MANAGEMENT

A model that illustrates how a hazard does not necessarily lead to injury or damage even though it presents a risk is given by King and Magid, and is the *pedestrian and banana skin* model [28]. A banana skin has been dropped on the footpath of a city street, immediately forming a hazard for pedestrians, who are at risk of and possible consequences caused by slipping on it. What are those possible consequences?

The first pedestrian sees the banana skin and avoids it, thus recognising risk and avoiding it. The second treads on it, skids and recovers. The third treads on it slips, recovers balance but drops and breaks a bottle of wine (leaving broken glass which increases the hazard and of course the risk) but is not injured. The fourth slips and suffers a minor injury, while the fifth falls heavily and is seriously injured (will either of them sue the city for damages?). These four have failed to recognise the risk presented by the banana skin and have accepted it, and the consequences, involuntarily.

It is suggested that there is a sixth case: the pedestrian who does not see the banana-skin and walks by without stepping on it, which illustrates that there is a difference between consciously avoiding a hazard (the first pedestrian) and inadvertently or involuntarily avoiding a hazard. The observation that the latter case exists has led this author to question the influence of what can only be called *blind luck* – or is it perhaps the notion of Kismet, that a person's fate is written on his/her forehead?

SUMMARY

We engineers do not reflect often enough that much of what we design and build have the capacities to be very effective killing devices, whether static items or machines-in-motion. Even if they do not kill, they can severely injure the person using them. As a reflection on that we offer, a collection of short stories, some of which is not particularly good fiction, in this author's opinion, but it suggests care needs to be taken when we design *anything* [29].

The many definitions and illustrations given above show the nature of risk and what engineers need to know of it in general. Then there are the particular areas of engineering practice, the areas in which engineers meet their work situations, and whether that work involves building a bridge (which may fall down and kill workers as the Westgate Bridge did while under construction in Melbourne, Australia) or building a nuclear power plant or even designing household appliances (which may injure a woman, as did two, in accidents which this author investigated). So it must be remembered that *things can go wrong*. The enormous difficulty is imagining *how* things can go wrong and this author has observed there are many who lack imagination. The most dangerous person in a design committee is the one who asserts: *Nothing can go wrong!* – and is believed.

The level of that need-to-know depends on many factors, for example, on whether the work being performed is of a markedly innovative nature, something involving new technology, or a shift in application of existing technology. In those cases and any similar, the risk is higher.

At the simplest level of explanation, it is all about not making mistakes. The best suggestion that can be offered for that and for risk acceptance and management is all-round awareness; better still, *spherical awareness*, not just around oneself but above and below also.

A CONCLUSION

A suitable conclusion to considering how to regard and treat risk, which is a very *iffy* subject, are these lines adapted and extended from a source that may be recognisable to many readers of this article:

> *Give me the competence to identify risks in my professional work, the education to assess and evaluate quantitatively and/or qualitatively how those risks may affect me, the common sense to avoid those risks which can be avoided, the serenity to accept the risks I cannot avoid, and the wisdom to tell which is which. Then the courage to control, mitigate or transfer those risks I have had to accept.*

Given all that, the possibility of litigation should be extremely remote.

REFERENCES

1. Ward, R.B., The Relationship between Hazards and Management Practices in the Chemical Industry. Unpublished PhD thesis, Department of Safety Science, University of New South Wales (1994).
2. Langbaum, F.L.V. (Ed.), *The Random House French Dictionary*. New York: Random House (1990).
3. Johnston, G. (Ed.), *The Australian Pocket Oxford Dictionary*. Melbourne: Oxford (1976).
4. Mondarres, M., *What Every Engineer Should Know About Reliability and Risk Analysis*. New York: Marcel Dekker (1993).
5. Institution of Professional Engineers, New Zealand, Engineering Risk. Wellington: Institution of Professional Engineers, New Zealand (1983).
6. Viner, D., *Accident Analysis and Risk Control*. Fairfield: VHMS (1991).
7. Steele, L.W., *Managing Technology: the Strategic View*. New York: McGraw-Hill (1989).
8. Engineering Practice Committee, Institution of Chemical Engineers, UK, Nomenclature for Hazard and Risk Assessment in the Process Industries. Rugby: Institution of Chemical Engineers (1985).
9. Center for Chemical Process Safety, Guidelines for Chemical Process Quantitative Risk Analysis (with Worked Examples). New York: Centre for Chemical Process Safety, American Institute of Chemical Engineers (1989).
10. Raman, R. and Cameron, I., Hazard and Risk Assessment, Course and Workshop. *Chemeca '89*, Gold Coast, Australia (1989).
11. Kletz, T.A., The application of hazard analysis to risks to the public at large. *Proc. 1st World Congress on Chemical Engng*., Amsterdam, the Netherlands (1976).
12. Withers, J., *Major Industrial Hazards: Their Appraisal and Control*. Aldershot: Gower Technical Press (1988).
13. Kuhlmann, A., Introduction to Safety Science. New York: Springer-Verlag (1986).
14. Miller, P., (Ed.), Are You at Risk? Canberra: Institution of Engineers, Australia, (1990).
15. Institution of Engineers, Australia, Dealing with Risk. Canberra: Institution of Engineers, Australia (1993).
16. Hines, W.W. and Montgomery, D.C., *Probability and Statistics*. New York: John Wiley & Sons (1972).
17. Slovic, P., Perception of risk. *Science*, 236, 17 April (1987).
18. DeLuca, D.R., Stolwijk, J.A.J. and Horowitz, W., *Public Perceptions of Technological Risks: a Methodological Study*. In: Covello, V.T., Menkes, J., and Mumpower, J. (Eds), Risk Evaluation and Management. New York: Plenum Press (1986).
19. Slovic, P., Fischhoff, B. and Lichtenstein, S., *The Psychometric Study of Risk Perception*. In: Covello, V.T., Menkes, J. and Mumpower, J. (Eds), Risk Evaluation and Management. New York: Plenum Press (1986).
20. Lowrance, W.W., *Of Acceptable Risk*. Los Altos: William Kaufmann (1976).
21. Fremlin, J.H., *Power Production: What are the Risks?* Oxford: Oxford University Press (1987).
22. Adams, J., *Risk*. London: UCL Press (1995).
23. Standards Australia, Risk Management AS/NZS 4360:1999. Sydney: Standards Australia (1999).
24. Ardis, P.M. and Comer, M.J., *Risk Management*. London: McGraw-Hill (1987).
25. Kendall, R., *Risk Management for Executives*. London: Pitman Publishing. (1998).
26. Wang, J.X. and Roush, M.L., *Risk Engineering and Mananagement*. New York: Marcel Dekker (2000).
27. Head, G.L., *The Risk Management Process*. New York: Risk Management Society Publishing (1978).
28. King, R.W. and Magid, J., *Industrial Hazard and Safety Handbook* (3rd edn). London: Butterworth (1982).
29. Saberhagen, F. (Ed.), *Machines That Kill*. New York: Tom Doherty Assoc. (1984).