Chapter 11
Risk in the design process

Chris McMahon
University of Bath

Jerry Busby
Lancaster University

Uncertainty pervades engineering design. There is variation in all materials and processes, in all engineering parts and assemblies. The use (and abuse) of engineering artefacts differs from user to user and there are large unknowns in the impact on the natural environment. Our understanding of the factors that influence artefact performance is incomplete, and our analytical and predictive methods are imperfect. We cannot predict all of the ways in which a process or an artefact might fail. We cannot completely replicate on the test bed or in prototype development the loads to which our designs will be subject in use. For these and for many other reasons engineering design is an uncertain activity, and thus a source of risk – of the possibility of an undesirable event or outcome.

11.1 The Paddington rail disaster
© PA photos

Undesirable outcomes in engineering can include poor technical or commercial performance of an artefact, danger to life and limb for a user of an artefact, or impact on the environment or some third party. Such outcomes have existed throughout the history of engineering, but today have acquired a particular importance because of the high cost and timescales and distributed nature of many engineering projects, the complexity and inherent danger of some engineering artefacts and systems, and the aversion of many people to personal and commercial risk.

The present importance of risk has led to a great deal of recent interest in its active management. This involves a number of techniques, ranging from general approaches to risk identification, assessment and monitoring through to analytical methods that represent and manipulate uncertainty in design parameters. Risk management has become a standard engineering technique, contractually required in many engineering projects. But while qualitative approaches to risk management have had some success, quantitative risk assessment has had a much lower impact except in very risk-sensitive domains such as nuclear engineering and aerospace.

It is also apparent that public and private attitudes to risk are not strictly informed by rational judgements of likelihood and impact, but also by perception, and in particular that risk perception is strongly influenced by dread and by dangers imposed by others. For these reasons perception has become an important factor in the engineer's consideration of risk.

This chapter will review all the aspects of risk and uncertainty in engineering that have been noted above. It will first provide an overview of the nature of risk and uncertainty in engineering, and will distinguish between different aspects of risk from the point of view of the engineer. It will then review current approaches to risk in engineering – first through an overview of approaches to risk assessment and management and then through a brief exploration of quantitative approaches to the evaluation of risk and uncertainty. It will finish with an overview of the impact of perception on risk in design, and a note of some aspects of risk management in practice.

The nature of risk and uncertainty in engineering

Risk in engineering design encompasses a variety of issues for a wide range of stakeholders. It encompasses risk to organisations in the product supply chain – manufacturers of parts, assemblies and integrated systems, maintainers and recyclers – to the customer or user of artefacts, and to the wider community both in the present day and in the future. It also involves a variety of concerns, which include:

- *Technical risk* – i.e. risk that the artefact will not perform as intended. Technical risks include, for example, the possibility that an aircraft will not reach its payload/range targets or that components of an automobile engine will fail prematurely.
- *Project risk* – i.e. risk that a project will fail or will overrun in cost or time. Examples of adverse outcomes in project risk include a military procurement contract that exceeds budget and a civil engineering occupation of a railway track that exceeds an allocated time period.
- *Risk to life and limb* – i.e. risk that someone will be killed or injured as a consequence of use or even abuse of the artefact. Examples include the risk of injury from failure of transportation devices or production equipment and also long-term hazards to health from asbestos insulation.
- *Risk to the environment, or to future generations*. Examples include risk of pollution from a manufacturing process or of depletion of scarce materials.

Risks exist in all aspects of life, but those associated with the manufacture or construction and use of engineering artefacts are often particularly acute.

Risks exist in all aspects of life, but those associated with the manufacture or construction and use of engineering artefacts are often particularly acute. The artefacts are in continual use in very large numbers: we all spend many hours of each day interacting with them (to the extent that they may be so familiar to us that we fail to show them the respect that they deserve), and the artefacts themselves often have a high propensity to cause injury or death as a result of the energies involved in their construction and use.

Complexity

Engineering artefacts are also often characterised by complexity in a number of respects. Many artefacts themselves are both complex and complicated, involving very many component parts and requiring significant skill and knowledge in their construction and use. In modern aviation systems, for example, individual aircraft may have in the order of a million component parts, and they interact with other aircraft, with airport and air traffic control systems (Figure 11.2) and so on. The number of potential failure modes is enormous, as is the number of modes of interaction between components and subsystems.

11.2 Air traffic control, part of a complex modern aviation system

Complexity in engineering also extends to the number and geographic distribution of the people and organisations involved in the design and construction of engineering artefacts. A design team can today be spread between three continents, as can the companies in the supply chain. This geographic distribution is necessary because the cost of large design and development programmes, such as those for aircraft or automobiles, is now so great as to require firms to collaborate in order to spread the development costs and achieve the necessary economies of scale. These costs also mean that the number of new product programmes in some areas is small, and therefore the implications of failure for the organisations concerned (including governments where these are the customers) can be severe.

A further aspect of complexity and coupling in engineering concerns the interactions between the engineered artefact and the natural environment. In this regard, hazards such as those imposed by extreme events including earthquakes, large waves or high winds are well known, but an emerging understanding is developing of the implications for the natural world of long-term use of engineering artefacts, owing to the interaction of man-made materials with the environment, the impact of pollutants and so on.

Human factors

Finally, and of considerable importance, people have a huge impact on risk in design. Many failures and uncertainties in the engineering process are due to human error, and there are many uncertainties in the way in which people may interact with an artefact, ranging from areas such as market acceptance of a new product and, in particular, unforeseen abuse of the artefact itself.

The subject has perhaps been investigated most widely by those concerned with the consequences of design error resulting in structural failure, and these have tended to concentrate on the nature and effect of human error. For example, Stewart (1992) suggests that reviews of statistical data indicate that up to 75% of structural failures are human errors, and suggests that human error also accounts for much of the discrepancy between estimated and actual probabilities of artefact failure. Petroski (1991) argues that human error is the most likely cause of fundamental errors made at a conceptual stage, which can be the most serious and elusive of design errors. Cambell (2002) suggests that some 30% of construction failures are due to design error, and emphasises the importance of education and quality systems that ensure all aspects of the design are thoroughly and independently checked.

Human error is also very significant in accidents and other undesirable outcomes resulting from the use of engineering artefacts. For example, it is estimated that 70% of aircraft accidents involve pilot error (and error by maintenance and other ground staff will contribute further), while 80% of shipping accidents involve human error (Hawkins, 1993; Lucas, 1997). Such bald statistics may, however, obscure the contribution that can be made by other factors even in cases that are ostensibly due to human error. Bennett (2001) argues that bad design, poor training, unrealistic rosters, substandard maintenance and other factors outside the control of the flight crew may often be significant in aircraft failures.

A similar picture may be found in UK National Health Service hospitals, where it is estimated that adverse events, in which harm is caused to patients, occur in around 10% of admissions – or at a rate in excess of 850,000 a year; and that these cost the service an estimated £2 billion a year in additional hospital stays alone. It is thought that human error may sometimes be the factor that immediately precipitates a serious failure, but there are usually deeper, systemic factors at work which, if addressed, would have prevented the error or acted as a safety net to mitigate its consequences (DOH, 2000).

Approaches to risk management

Although risk pervades engineering, designers have traditionally used very limited tools to assess the likelihood and impacts of risks.

Although risk pervades engineering, designers have traditionally used very limited tools to assess the likelihood and impacts of risks. Engineering calculations have generally been deterministic, with uncertainty taken account of through so-called "factors of safety". Project risk has often been dealt with simply by trying to identify likely risk factors and to take steps to mitigate them.

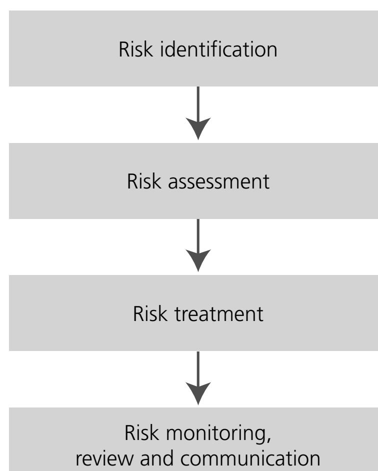
The past 20 years have, however, seen a significant change in attitude to risk for the reasons noted above: the complexity of modern engineering projects is such that the investment in time and money in new product development is large; and a single product failure may have a major impact on a company. Projects are often distributed between companies and often between countries, and risk has to be formally managed within the frameworks for collaboration. There is a much more widespread use of fixed-price contracts, especially by government. Consumer awareness has put an increased emphasis on safety and reliability, and customers and others impacted by products have become increasingly litigious: we are living in a "risk society" (Lupton, 1999). There has also been an increasing awareness of the impact of artefacts on the environment, and of other external impacts such as that on national economies (Kammen and Hassenzahl, 2001). There exists also risk relating to everyday interactions, particularly within the work place (Bloor, 1995).

Risk management is defined as "co-ordinated activities to direct and control an organisation with regard to risk."
(ISO/IEC, 2002)

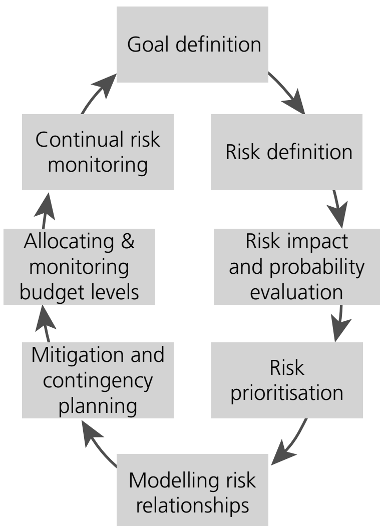
The changes in attitudes have been reflected in developments both in design practice and in research in design and in the social sciences. Formal risk management has become a requirement for a significant number of projects, in particular those financed from public funds (MOD, 1996a). Many more companies incorporate risk management in their procedures, both for project and technical risk, although not contractually required to do so (Crossland *et al.*, 1998, 2003). New techniques have been developed for project and technical risk assessment and management. These include a number of risk management methodologies (Carter *et al.*, 1994; Simon *et al.*, 1997; ICE, 1998; Patterson *et al.*, 1999), and software tools for risk management and assessment (@Risk; Monte Carlo; CIRIA; BSI, 1991; Kletz, 1992).

In the ISO guide to risk management vocabulary (ISO/IEC, 2002), risk management is defined as "co-ordinated activities to direct and control an organisation with regard to risk". There are many published methodologies prescribing an idealised generic process for risk management, including that published by the Risk Special Interest Group of the Association for Project Management (Simon *et al.*, 1997), Chapman and Ward's (1997) nine-phase generic risk management process structure, and the Riskman methodology (Carter *et al.*, 1994). All of these are intended to provide a framework for risk analysis and control, rather than a detailed prescription of techniques. Nevertheless, the four key phases (Figure 11.3) in all such risk management processes are (MOD, 1996b, c; DOD, 2000; ISO/IEC, 2002):

- *Risk identification* – the process of finding, listing and characterising elements of risk.
- *Risk assessment* – the overall process of risk analysis and risk evaluation.
- *Risk treatment* – the process of selection and implementation of measures to modify risk.
- *Risk monitoring, review and communication* – a continual process of re-examining assumptions, reviewing developing risk and communicating likely impacts to stakeholders.



11.3 The four key phases of the risk management process



11.4 A general risk management process (Crossland *et al.*, 1998)

The risk management cycle

The four key phases identified above may be expanded into a cyclic sequence of risk identification, prioritisation, monitoring and review, representing a plan for risk management action, as shown in Figure 11.4. The stages of this cycle are broadly as follows.

Goal definition: identification of measurable control parameters and determination of a base plan (the planned structure of project elements if no risk events occur) and risk management plan. The identified and recorded risks represent deviations from this plan.

Identification of both risks and opportunities, and of the members of the project team who are most closely concerned with those risks (the "owners"). The tools and techniques used for risk identification include questionnaires, checklists, prompt lists, expert interviews, formal risk review procedures, workshops, brainstorming, risk response analysis (Cooper and Chapman, 1987) and knowledge-based systems (KBS) (Niwa, 1989; Cailleaud *et al.*, 1999). Identified risks are recorded in a risk register (Carter *et al.*, 1994) or risk list (CCTA, 1995).

Risk impact and probability evaluation: the impact and probability of risks is identified and recorded. Numerical evaluations are given wherever possible, and recorded in the register. Techniques for analysing and evaluating the probability and impact of identified project risks include schedule-specific techniques such as the critical-path method, Gantt charts and the program evaluation and review technique (PERT) (Moder and Phillips, 1970; Starkey, 1992), qualitative techniques such as probability/impact matrices and use of high/medium/low categories for probability and for impact (Carter *et al.*, 1994; Coppendale, 1995). Equivalent techniques for technical risk include failure mode and effects analysis (FMEA), hazard and operability (HAZOP) and preliminary hazard analysis (PrHA).

Risk prioritisation: the evaluated impact and probability for each identified risk are used to determine which risks should be included in the risk model.

Modelling relationships: relationships are modelled in terms of time, cost, performance or other measures. Some methodologies reduce everything to cost.

Mitigation and contingency: the base plan is changed to reduce probability or impact. Contingency plans are triggered and trade-offs identified.

Budgets are allocated and monitored for measurable/controllable parameters.

Risk monitoring of the identified risks takes place. Probabilities and impacts are updated. New risks arise. Existing risks are eliminated. Trigger events are monitored. The risk monitoring activity in turn contributes to the next cycle of risk identification, prioritisation and monitoring, so closing the loop.

Risk management in practice

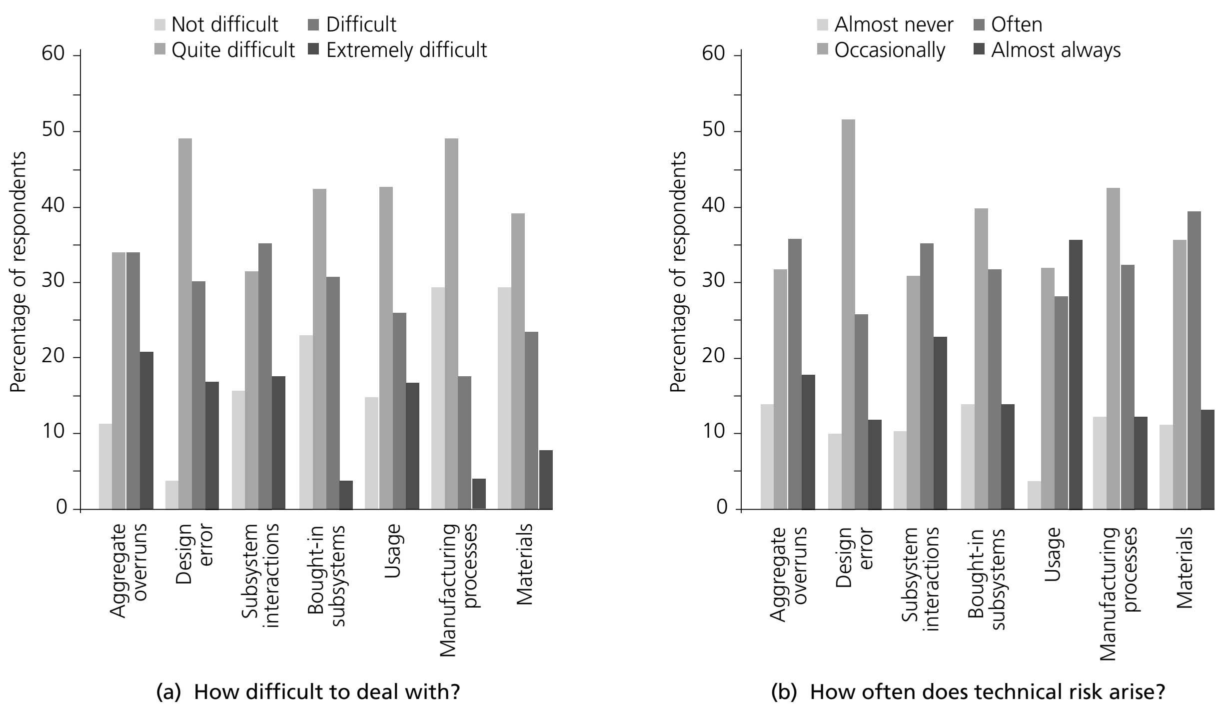
A number of industries have been at the forefront of developments in risk management. A good deal of the early focus was on risk to life and limb, especially in high-impact industries such as nuclear, aerospace and construction, and these industries have remained a strong focus of risk research. So far as project and technical risk are concerned, a good deal of work on design project risk management has concentrated on the design of software systems (Boehm, 1991; Ould, 1999), which seems to be inherently more technically risky than many other kinds of design. The defence and construction industries (Edwards, 1995; Godfrey, 1995) have also been at the focus of formal project risk management methods, owing to the sheer size of their projects. Issues of technical risk have also been particularly important in defence programmes, owing to the rapid pace of technical change combined with long programme timescales (MOD, 1996a – c). Technical risk is also at the forefront of concerns in aerospace, nuclear and medical engineering, where the impact of failure is particularly high (Health and Safety Executive, 1992; FDA, 2000; Ward and Clarkson, 2004), and in construction programmes such as the design of flood and coastal defences owing to the unpredictable nature of natural forces and the long timescales involved (Godfrey, 1995). Both uncertainty and risk issues are paramount in the oil and gas sector, where a single decision determines massive financial investment. There are huge uncertainties regarding what lies beneath the ground and there are huge health and safety issues, for example Piper Alpha and Exxon Valdez (Heising and Enzenbach, 1991; Aven and Pitblado, 1998; Bea, 1998).

With the increasing use of analysis and simulation techniques in engineering it is very important for engineers to understand the uncertainties and risks inherent in the use of such techniques. Computer models in engineering design are representations of products or processes that may be prone to uncertainty, variability or error. There is a need for approaches that help engineers understand the nature of such variability and identify whether models are appropriate for specific uses. In this regard, a number of approaches for the evaluation of the suitability of techniques have been devised – for example, Rajabally *et al.* (2003) propose a methodology that uses Bayesian belief nets to capture the reasoning associated with justifying model trustworthiness and Balci (2001) proposes a systematic approach for the evaluation of hierarchies of direct and indirect indicators and the aggregation of indicator scores. These approaches depend on expert assessment of techniques – often there is a lack of well organised verification data – the organisation and accumulation of such data is an important future research issue.

With the increasing use of analysis and simulation techniques in engineering it is very important for engineers to understand the uncertainties and risks inherent in the use of such techniques.

A workshop on issues in engineering risk assessment and perception held at the University of Bristol in 2002 (McMahon *et al.*, 2002) suggested that identifying potential risks is seen as particularly important in an industrial context. The consensus was that where a risk is identified, then the assessment and mitigation carried out are generally effective. The identification of a potential risk in the first place is the weakest part of the process. One problem is that those who experience failures of the product (for example, disgruntled users, seriously injured or relatives of deceased) are often not on good terms with those who make or specify the product. There is reluctance to contact such people to gather information, and yet they often have unique stories to tell.

Crossland **et al**. (1998, 2003) carried out a survey of risk management practice in UK engineering companies. In one part of the survey, respondents were asked to identify the difficulty of dealing with different sources of technical risk. As shown in Figure 11.5a, the aspects considered "difficult" or "extremely difficult" to deal with by the most respondents were (in descending order) aggregate budget overruns (where budgets include cost,



11.5 Risk management survey results

weight, *etc.*), design errors, subsystem interactions and product usage (understanding the loads and usage that a product will be subjected to during its life). Respondents were also asked how often technical risk arises in each area, and here usage, subsystem interactions, materials and aggregate overruns were the most important areas, as shown in Figure 11.5b.

The survey covered a number of other topics, and is reported in full in Crossland *et al.* (1998). Perhaps the most important conclusion from the work from the point of view of future design methodologies is that, while many companies collect data about risk, the incorporation of quantitative models into risk management is rare. Improved techniques are needed to link together data collection with predictive and modelling methods.

Risk in teams

We have noted that engineering is more than ever carried out by large teams, usually distributed between several organisations and often separated by substantial distances. Many of the difficult aspects of engineering risk come from the complexity associated with these large teams. We have also noted that risk is difficult to assess and control where it arises from subsystem interactions, from interactions between participant groups in a project, and from aggregate budgets – where, for example, the responsibility for the weight budget or cost budget for an artefact is spread amongst many participants in a project. Understanding of the risks and uncertainties in a project or in the performance of an artefact will also be distributed amongst the members of a team – in this case the issue is one of communicating this understanding to those responsible for decision making.

Many of the difficult aspects of engineering risk come from the complexity associated with large teams, usually distributed between several organisations and often separated by substantial distances.

In all of these cases, a major issue in risk assessment and management concerns the provision of methodologies that allow members of a team to collaborate in building a shared understanding of risks and uncertainties. Examples of research issues include:

- How can the team accumulate an understanding of the risks and uncertainties associated with the processes and activities that they undertake, particularly to accumulate evidence about the uncertainties inherent in analytical and simulation methods?
- How can the team record its view of the risks and uncertainties arising from subsystem and group interactions and emerging aggregate budgets?
- Can an environment be provided that allows team members to flag up and record their concerns in a confidential manner?

The quantitative evaluation of risk and uncertainty

The most widely used approaches to quantitative analysis of risk are firmly grounded in probability.

Although a good deal of risk management is still qualitative, the quantitative assessment of risk is a significant engineering objective, and a number of techniques have been developed to support this. These techniques are also closely allied to the development of more general approaches to design analysis under uncertainty. The most widely used approaches to quantitative analysis of risk, and of uncertainty more generally, are firmly grounded in probability, although fuzzy systems have had an impact, as have some other techniques. For all approaches, introduction has been facilitated by vastly improved computing capabilities.

The main quantitative risk assessment techniques applied in risk assessment include (Andrews and Moss, 2002):

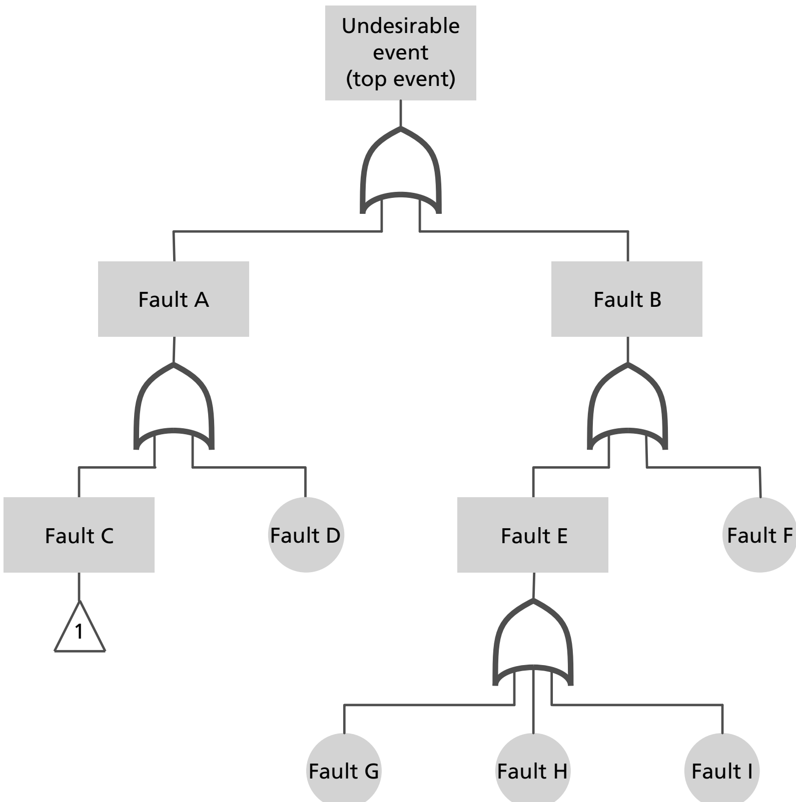
Fault tree analysis (Schneeweiss, 1999a, b). This is a graphical technique in which occurrences in a system which can result in an undesirable outcome are described in the form of an inverted tree. The most serious outcome, such as explosion, toxic release, *etc.*, is selected as the top event of the tree, and then the remainder of the tree, constructed by considering the sequence of events which individually or in combination could lead to the top event. The construction of the tree allows the probability of contributory events and the logic of event combination to be considered.

Event tree analysis. This is again a graphical technique, used to analyse the consequences arising from a failure or undesired event. An event tree, by contrast, begins with an initiating event, such as a component failure, and then considers consequences of the event through a series of possible paths, where each path is assigned a probability of occurrence. In this way the probability of the various possible outcomes can be calculated.

Decision tree analysis. As the name implies, decision trees are again a graphical technique, but in this case the branching of the tree reflects both choices of action that may be taken and chance events, and the numerical values assigned to the branches reflect probabilities and values of outcomes.

Influence diagrams use more general graphs, in which the nodes represent variables or decisions, and the edges indicate the path or direction in which one node can influence another. Influence diagrams can be used as a basis for decision trees, but can also model more subtle and sophisticated relationships and are perhaps the most general of the diagrammatic techniques.

FMEA. This is a technique that aims to identify potential ways in which a product or process might not meet expectations and any possible causes of such failure, and to rank failures and their causes to indicate where



11.6 Fault tree analysis, a graphical tool for risk assessment

engineering effort should be expended to reduce failure likelihood and severity. The basis of FMEA is to try to identify and list all possible ways in which an assembly, a part or a process might fail. For each possible failure mode an assessment is made of the severity should failure occur and possible causes of the failure. For each cause, assessment is made of the likelihood of its occurrence and the likelihood of detection. The three assessments – severity, occurrence and detection – are then multiplied together for each failure mode/cause to give a risk priority number (RPN) which is used as an aid to indicate the priority of action for each mode.

Technical risk assessment tools include all of the techniques mentioned so far, as well as safety factors and a number of reliability techniques, in particular based on limit state analysis and the first- and second-order reliability methods (FORM and SORM) (Hasofer and Lind, 1974; Fiessler *et al*., 1979). Limit state theory provides the framework within which the performance of engineering components can be assessed against various limiting conditions, e.g. a

Monte Carlo analysis is extensively used in technical risk assessment for simulations involving extensive computation.

Traditionally, designers have often used deterministic analysis combined with safety factors to manage risk.

condition of load exceeding resistance in a structure such that the component is no longer able to fulfil its intended function. In the FORM, the limit state is linearised around the design point, the point on the limit state with the highest probability. FORM has the advantage of simplicity, but in highly non-linear situations and as the degrees of freedom of the problem increase it may be subject to increasing error. The SORM is constructed by fitting a parabolic surface (as opposed to a plane surface in FORM) to the limit state function at the design point. The information about the curvature of the limit state function is utilised in SORM, therefore improving results from FORM.

Monte Carlo analysis (Hammersley and Handscomb, 1964) is extensively used in technical risk assessment and probabilistic analysis for simulations involving extensive computation. Where the performance function is computationally expensive (for example, with finite element analysis), techniques such as the response surface method (Bucher and Bourgund, 1990), in which an approximate mathematical function of the performance function is used to avoid computations of the actual performance function, minimise the computation required. Advanced mean value (Wu *et al.*, 1990) and fast probability integration (Wu and Wirsching, 1987) are further approximate techniques designed to achieve good results for computationally intensive situations.

Other methods

There are many other quantitative methods for risk and uncertainty analysis in design. Traditionally, designers have often used deterministic analysis combined with safety factors; in the absence of information about statistical probabilities for design variables, techniques such as interval analysis (for example, applied in tolerance stack analysis) and the absolute worst-case variation (in which the variables are either set to the lowest or largest expected value) are used. Fuzzy theory has had some application in risk assessment, but the use of fuzzy methods is most appropriate in manipulating design imprecision in earlier design phases, whereas probabilistic design is most suited to problems with stochastic uncertainty (Wood and Antonsson, 1989).

Industrial application of quantitative methods

The Society of Automotive Engineers (SAE, 2003) reports the following barriers to implementation of probabilistic methods:

1. the methods are a radical departure from existing practices;
2. they are not compatible with existing tools;

3. they are too difficult to use and take too long;
4. they take too much data;
5. the results from probabilistic methods cannot be verified and output data is difficult to interpret;
6. the complexity of multiple failure modes is an issue.

They also note the following limitations of probabilistic methods:

1. lack of guidelines for dealing with remote probabilities;
2. lack of guidelines for data adequacy;
3. lack of guidelines for model adequacy;
4. difficulty in validation;
5. required deterministic calculations can be too expensive;
6. failure modes are often poorly identified;
7. difficulty in negotiating risk limits.

Our experience in exploring the use of probabilistic methods in component life assessment is that many of these issues are important, but by far the biggest difficulties, at present, concern the lack of sufficiently complete data (and associated data and model guidelines) for the application of the method – for example, in automobile engineering the necessary data would include that on road conditions, driver behaviour, material properties and the effects of treatment (for example, on residual stresses), the behaviour of tyres and bushes and so on. And even if a full set of data were available on all aspects of the design problem, there would still be limitations in our understanding of the uncertainty inherent in the analytical techniques. This suggests the need for a database framework that would allow information to be collected and collated for use in risk and uncertainty evaluation.

Even if a full set of data were available on all aspects of a design problem, there would still be limitations in our understanding of the uncertainty inherent in the analytical techniques.

Risk perception

Risk to life and limb has always been of particular concern to engineers, and many of the quantitative approaches to risk and much of the legal and regulatory emphasis on risk have concerned such hazards. However, it is now increasingly recognised that the separation between the objective and subjective in risk is difficult to maintain – it is also accepted that all knowledge of risk has an element of subjective judgement. The subjective is particularly important in judging the societal impacts of hazards.

A central problem, however, lies in the discrepancies between the analytical frameworks used by designers to determine risk, and the qualities of a risk that actually influence risk bearers. Design risk analyses assess probability and impact, whereas lay people appear to perceive risk on the basis of a variety of factors that give them a richer picture of what a risk means to them. These factors include dread (lack of control, catastrophic potential, inequitable distribution, *etc.*) and the extent to which a risk is unknown (being new to society, being delayed in its effects, *etc.*) (Slovic, 1987). They seem to be influenced by various cultural biases (Adams, 1995) and the information they receive about risk is mediated by a range of social mechanisms (Kasperson *et al.*, 1988).

An important impact of risk perception is that people often overestimate the risk associated with very low probability events, and underestimate that associated with high probability events. As an illustration of this issue, consider Lomborg's (2001) observation that "if we drink water which contains pesticides at the EU limit value for a whole lifetime, we face the same death risk as if we smoke 1.4 cigarettes, cycle 15km, live two months in a brick building or drink a half litre of wine – just once". If we asked people what they perceived to be the risk from these various sources, we would surely get a very different view of the relative risks inherent in the different activities.

People often overestimate the risk associated with very low probability events and underestimate those associated with high probability events.

There is a basic question about whether design, in the service of society, should replace society's inexpert risk assessment with its own conception of what is rational – or whether it should incorporate in its own risk assessment models some of the dimensions that influence risk bearers. If the former, then designers need to communicate and influence users more effectively, and there are basic questions as to how to do this. If the latter, then there are some difficult questions about how qualities like dread should be incorporated in risk analyses in sensible ways.

Risk perception is intimately associated with attitudes to risk and acceptance of risk, and has been the subject of study from a number of perspectives, including the psychology and sociology of risk and the economics of risk (Pidgeon, 1999; Slovic, 2000). Perception is part of the management of risk – people think of risk management as risk reduction, but this is not always possible (Sandman ***et al.***, 1997). It is associated with risk communication: through the supply chain, right through to honesty with the public. The issue is how to communicate the residual risk. Psychology and issues of the man–machine interface also have a strong place in studies of error and hazard – human and organisational factors cause up to 80% of risks – and in their impact on health and safety issues.

Conclusion

A number of factors have contributed to the present emphasis on risk in engineering design. We live in a world of complex, interacting engineered systems. The design process is itself often complex, with many, distributed participants working over long time periods to bring products to market. The cost of the process may be high, and the financial implications of failure significant. And both the users of engineering products and the wider community are much more averse to risk arising from engineering design than before – in particular to life and limb, but also commercial and technical risk.

This article has reviewed some of the responses that have been made to the need to manage risk actively. It has introduced the nature of the risk management cycle, has outlined some of the qualitative and quantitative techniques that can be applied in risk assessment and monitoring, and has given an overview of their impact in practice. From this review it has been noted that, while many approaches have been developed, the application of quantitative risk management in practice is limited, and human error, both in designers and in users of their products, remains a significant issue. Furthermore, there is a limit to the extent to which quantitative approaches can be applied owing to the importance of societal attitudes to risk and to acceptance of risk. The engineering designer must take an approach that considers both the formal assessment of risk and the implications of societal risk perception.

References

@Risk Palisade Europe.

Adams J (1995) Risk. UCL Press

Andrews JD, Moss TR (2002) Reliability and risk assessment, 2nd Edition. Professional Engineering Publishing

http://www.palisade-europe.com/html/decisiontools_suite.html

Aven T, Pitblado R (1998) On risk analysis in the petroleum activities on the Norwegian and UK continental shelves. Reliability Engineering and System Safety, 61(1/2): 21–29

Balci O (2001) A methodology for certification of modelling and simulation approaches. TOMACS, 11(4): 352–377

Bea R (1998) Human and organisational factors in the safety of offshore structures. Reliability Engineering and System Safety, 61(1/2): 109–126

Bennett S (2001) Human error – by design. Perpetuity Press

Bloor M (1995) The sociology of HIV transmission. Sage

Boehm BW (1991) Software risk management: principles and practices. IEEE Software, 8(1): 32–41

BSI (1991) Reliability of systems, equipment and components. BS 5760: PART 5. http://www.bsi-global.com

Bucher CG, Bourgund U (1990) A fast and efficient response surface approach for structural reliability problems. Structural Safety, 7: 57–66
Caillaud E, Gourc D, Garcia LA, Crossland R, McMahonC (1999) A framework for a knowledge-based system for risk management in concurrent engineering. Concurrent Engineering Research and Applications, 7(3): 257–268
Cambell P (2002) Learning from construction failures: applied forensic engineering. John Wiley
Carter B, Hancock T, Morin J-M, Robins M (1994) Introducing RISKMAN methodology: the European project risk management methodology. NCC Blackwell
CCTA (1995) An introduction to managing project risk. HMSO
Chapman CB, Ward S (1997) Project risk management: processes, techniques and insights. John Wiley
CIRIA RiskCom. http://www.ciria.org.uk/
Cooper DF, Chapman C (1987) Risk analysis for large projects: models, methods and cases. John Wiley
Coppendale J (1995) Manage risk in product and process development and avoid unpleasant surprises. Engineering Management Journal, 5(1): 35–38
Crossland R, McMahon CA, Sims Williams JH (1998) Survey of current practice in managing design risk. University of Bristol
Crossland R, McMahon CA, Sims Williams JH (2003) The practical application of design risk assessment models. IMechE, Part B, 214: 227–234
DOD (2000) Military standard 882D – standard practice for system safety. US Department of Defence. http://www.reliasoft.org/mil_std/mil_std_882d.pdf
DOH (2000) An organisation with a memory – report of an expert group on learning from adverse events in the NHS, chaired by the Chief Medical Officer. UK Department of Health. http://www.doh.gov.uk/orgmemreport/
Edwards L (1995) Practical risk management in the construction industry. Thomas Telford
FDA (2000) Medical device use-safety: incorporating human factors engineering into risk management. http://www.fda.gov/cdrh/humfac/1497.html
Fiessler B, Neumann H, Rackwitz R (1979) Quadratic limit states in structural reliability. Journal of Engineering Mechanics Division, 105(EM4): 661–676
Godfrey PS (1995) Control of risk: a guide to the systematic management of risk from construction. CIRIA

Hammersley JM, Handscomb DC (1964) Monte Carlo methods. Methuen
Hasofer M, Lind NC (1974) Exact and invariant second-moment code format. Journal of Engineering Mechanics Divisions, 100(EM1): 111–121
Hawkins FH (1993) Human factors in flight. Ashgate
Health & Safety Executive (1992) The tolerability of risk from nuclear power stations. HSE Books
Heising C, Enzenbach W (1991) The ocean ranger oil rig disaster: a risk analysis. Risk Analysis, 9(1)
ICE (Institute of Civil Engineers and Institute of Actuaries) (1998) Risk appraisal and management for projects (RAMP). Thomas Telford
ISO/IEC Guide 73 (2002) Risk management – vocabulary – guidelines for use in standards. International Organisation for Standardisation
Kammen DM, Hassenzahl DM (2001) Should we risk it? Princeton University Press
Kasperson R, Renn O, Slovic P *et al.* (1988) The social amplification of risk: a conceptual framework. Risk Analysis, 8(2): 177–187
Kletz TA (1992) Hazop and Hazan identifying and assessing process industry hazards. Rugby Institution of Chemical Engineers
Lomborg B (2001) The skeptical environmentalist. Cambridge University Press
Lucas D (1997) The causes of human error. In: Human factors in safety critical systems. Butterworth-Heinmann
Lupton D (1999) Risk (key ideas). Routledge
McMahon CA, Bennett S, Busby JS, Barr G (2002) Risk perception and assessment in design, research review and priority setting exercise. University of Bristol
MOD (1996a) Ministry of Defence: initiatives to manage technical risk on defence equipment programmes. Report HC 361, UK National Audit Office
MOD (1996b) Defence standard 00-56(PART 1)/2 – safety management requirements for defence systems - Part 1: requirements. UK Ministry of Defence. http://www.dstan.mod.uk
MOD (1996c) Defence standard 00-56(PART 2)/2 – safety management requirements for defence systems – Part 2: guidance. UK Ministry of Defence. http://www.dstan.mod.uk
Moder JJ, Phillips CR (1970) Project management with CPM and PERT. Van Nostrand

Monte Carlo for Primavera systems Inc.
http://www.primavera.com/products/p3_montecarlo.html
Niwa K (1989) Knowledge-based risk management in engineering: a case study in human–computer cooperative systems. John Wiley
Ould M (1999) Managing software quality and business risk. John Wiley
Patterson FD *et al.* (1999) Managing the risks within automotive manufacturing. Risk Management, 1(3): 7–23
Petroski H (1991) Paconius and the pedestal for Apollo: a case study of error in conceptual design. Research in Engineering Design, 3: 123–128
Pidgeon NF (1999) Social amplification of risk: models, mechanisms and tools for policy. Risk, Decision and Policy, 4(2): 145–159
Rajabally E, Sen P, Whittle S, Dalton J (2003) Combining evidence to justify the appropriate use of models in engineering design. ICED'03, Stockholm, Sweden
SAE (2003) Society of Automotive Engineers. G-11 Probabilistic Methods Committee. http://www.sae.org
Sandman PM, Weinstein ND, Hallman WH (1997) Communications to reduce risk overestimation and underestimation. Risk Decision and Policy, 2: 1–16
Schneeweiss WG (1999a) Advanced fault tree modelling. Journal of Universal Computer Science, 5(10): 633–643
Schneeweiss WG (1999b) The fault tree method (in the fields of reliability and safety technology). Hagen
Simon P, Hillson D, Newland K eds (1997) Project risk analysis and management guide (PRAM). Association for Project Management
Slovic P (1987) Perception of risk. Science, 236: 280–285
Slovic P (2000) The perception of risk (Risk, Society and Policy Series). Earthscan Publications
Starkey CV (1992) Engineering design decisions. Edward Arnold
Stewart MG (1992) Simulation of human error in reinforced concrete design. Research in Engineering Design, 4(1): 51–60
Ward JR, Clarkson PJ (2004) An analysis of medical device-related errors: prevalence and possible solutions. Journal of Medical Engineering and Technology, 28(1): 2–21
Wood KL, Antonsson EK (1989) Computations with imprecise parameters in engineering design: background and theory. Transactions of the ASME, 111: 616–624

Wu YT, Millwater HR, Cruse TA (1990) Advanced probabilistic structural analysis method for implicit performance functions. American Institute of Aeronautics and Astronautics Journal, 28(9): 1663–1669
Wu YT, Wirsching PH (1987) New algorithm for structural reliability estimation. Journal of Engineering Mechanics, 113: 1319–1336