# Risk analysis—a subjective process

In everyday life we make intuitive decisions without consciously attributing either quantitative or qualitative values to the risks involved. But in public policy and the deployment of modern technology, decisions need to be more 'objectively' informed, and for this risk analysis is used

by Felix Redmill

Risk analysis is often assumed to be objective, and its results—risk values and the decisions based on them—to be correct. Yet all stages of the process, including the techniques used, involve subjectivity. Always there is uncertainty, the need for judgement, considerable scope for human bias, and inaccuracy. The results obtained by one risk analyst are unlikely to be obtained by others starting with the same information.

There is also a natural impediment to arriving at 'correct' risk values. The future is implicit in risk, which does not define a current problem or a future certainty, but the potential for future harm. Thus, risk may be estimated but not measured, and its values cannot be assumed to be correct. The United Kingdom Interdepartmental Liaison Group on Risk Assessment (UK-ILGRA) recognises this in saying that risk assessment is 'a tool for extrapolating from statistical and scientific data' to arrive at 'a value which people will accept as an estimate of the risk attached to a particular activity or event'[1]. Pertinent questions are whether the estimate is a sufficiently good approximation for the purpose in hand, and what confidence there is in it.

Speaking of risk determination in technological systems, Lowrance pointed out that estimates of risk, whether made by scientists or lay people, cannot escape containing elements of subjectivity[2]. These, he said, enter into 'the very defining of the questions, and into the designing of the experiments used in assembling evidence, and then into the weighing of the social importance of the risk.' It is often claimed that the greatest value of risk analysis lies not in the values derived but in the fact that the process forces us to think deeply about, and therefore better understand, the risks.

Wharton advises us that, 'Failures to cope with uncertainty in the management of technological risk abound. Their causes include overconfidence in scientific knowledge, the underestimation of the probability or consequences of failure, not allowing for the possibility of human error and plain irresponsibility concerning the potential risk to others.'[3] He goes on to say, 'And yet to avoid such risks by adopting an overly conservative attitude to technological innovation may be to deny the potential benefits to shareholders, employees and society.' Indeed, achievement depends on accepting risks, and this is the reason for risk analysis—we need to understand the risks, so as to make informed decisions. Thus, we should recognise and allow for the subjectivity inherent in our analysis and decision-making.

The purpose of this article is to show the subjectivity in the process of risk analysis. This is not intended as a destructive dissection, for a major benefit of risk analysis is its subjectivity—its requirement for thought and judgement. It should not be the mere application of a set of rules. However, where subjectivity is arbitrary and could be reduced, or where its better understanding could improve accuracy, its exposure could be beneficial. Understanding their own subjec-

tivity and scope for error could lead risk analysts to recognise their assumptions and consider more fully the confidence that they can reasonably have in their results. It could also lead to research into the processes and techniques of risk analysis.

The first in a series of articles on the subject, this article addresses the overall process of risk analysis; subsequent articles will address the techniques used in hazard analysis, and the limitations of risk analysis when humans are its subject.

## The process of risk analysis

In most literature, risk analysis is divided into three stages or sub-processes:

- hazard identification
- hazard analysis
- risk assessment (or evaluation).

The purpose of the first stage is to identify the hazards that could lead to breaches of safety. That of the second is to analyse the identified hazards, estimate the frequency and severity of potential harm, and thus define the risks that they pose. The third stage assesses the risks against defined criteria so as to determine their tolerability.

The terms 'risk analysis' and 'risk assessment' are not consistently defined. They are used differently by different authors, and sometimes they are used synonymously or interchangeably. Here 'risk analysis' refers to the total process and 'risk assessment' to its final stage.

Risk analysis is 'generic' and may be applied to any situation and any form of decision-making, from determining policy and strategy, through all levels of planning, to tactical decision-making. The nature of the application and the purpose of the analysis influence the level of formality, the techniques used, and whether a quantitative or a qualitative approach is taken. Thus, it is both useful and important to define a planning, or 'definition of scope', stage to precede the three technical stages defined above.

## Definition of scope

The definition-of-scope stage necessarily involves the judgement of those planning the analysis. It influences the nature and direction of the analysis, and it is a predisposing factor on its results. Decisions must be made about the study itself and the system to be studied, and both sets of decisions involve considerable discretion. Kasper says, 'The very choice of questions to be asked, issues to be considered, and methods to be used involves judgement.'[4]

The terms of reference of a study place limitations on what sources of information are admissible and on where information may be sought. How a study is conducted (regardless of the terms of reference) can have the same effects. For example, if the public is not consulted, certain perspectives and opinions, and perhaps the main sources of opposition to a proposal, may be precluded. Wynne reports on how the Windscale Public Inquiry in 1977 was predisposed toward the evidence of the 'experts' and how this set the project's opponents at a disadvantage.[5,6]

The physical and logical boundaries of the 'system' to be analysed, whether it is a tangible system or a proposed policy, need to be defined. Then the analysis should identify and analyse the risks that may be posed to people, property or the environment on the other side of the boundaries. These, in turn, depend on the inputs and outputs across the boundaries, some of which may only be observable from some perspectives, or acknowledged by some participants, so any constraint on what data is acceptable, where it is sought, or who should provide it could severely affect the results.

The terms of reference may also place an outer boundary on the scope of the analysis. If, as in many cases, the system is an industrial plant, and the study is limited to the risks posed within the factory, then, by definition, any risks to the public are not considered. Similarly, risk analyses may be limited to one type of risk, say financial risks that management are interested in, while excluding other types, say safety risks that the public may be more concerned about.

However accurate the technical aspects of a risk analysis may be, the results are predisposed, or distorted, by the definition of the terms of reference, the exclusion of certain types of evidence, the definition of the study and system boundaries, and, in general, by the strategic planning of the analysis itself. Risk-tolerability decisions to be taken in the fourth (risk assessment) stage of the analysis are also influenced by the subjective first stage, for criteria against which they will be made should be defined then. Decision-makers need to be identified, the decision-making process defined, and its mechanisms put in place. If politicians, the public, or other non-experts are

to be involved, plans need to be made about what risk information will be communicated to them, and how and when it will be communicated. Subjectivity cannot be avoided.

**Hazard identification**

The purpose of this activity is to identify the sources of risk: the things that can go wrong and lead to breaches of safety. The nature of the hazards depends on the circumstances. For example, in an industrial plant hazards might include failures of equipment, human error, and the use of equipment outside its design specification, whereas in the formation of high-level policy they may be the potential causes of societal impact or environmental problems. In any case, the aim of the activity is to maximise the identification of hazards.

There are many techniques for hazard identification, and all depend on human observation, judgement, and creativity. As well as being key attributes of an effective study, these also introduce subjectivity and therefore the potential for bias.

A rudimentary means of hazard identification consists simply of pondering the circumstances, and this may be adequate in a low-risk situation. But in the fields of industrial and environmental safety, where risks are high and it is expected that professionalism, both in the relevant field and in hazard identification, should be brought to bear, a number of techniques have been developed.

In some well understood situations or systems, the use of a checklist may be adequate. For example, the annual Ministry of Transport (MOT) safety check of motor vehicles is based on testing, against predefined criteria, a list of components that would be hazardous if in poor condition. However, the adequacy of a checklist depends on a thorough understanding on what could go wrong. Without extensive past experience and documented fault and hazard histories, a checklist is not soundly based. Moreover, its adequacy also depends on the circumstances of its use being the same as those in which it was created; if they differ, the checklist could be out of date, or inapplicable, and dangerously misleading. Checklists, even when appropriate, need to be reviewed

periodically (the MOT checklist has been updated many times).

In systems which are not so well understood, perhaps because they are only now being planned or designed, techniques which employ the creativity of human investigation are required. Brainstorming is sometimes used, but although it is creative there is usually little formality in the process. Information for hazard identification may also be derived from audits and formal or informal interviews with staff, all of which depend on human abilities, attitudes and thoroughness.

The most powerful method in use today is HAZOP (hazard and operability studies), first developed in the chemical industry and later extended for use with systems involving software[7,8]. In recognition of the fact that no individual is likely to identify all possible hazards, this technique calls for a number of viewpoints to be represented. Not only is a team essential, but study planning, team leadership, and process formality are crucial to efficiency and the effectiveness of hazard identification.

Yet, ironically, the features essential to success can also be the seeds of failure. A HAZOP study can be lengthy (in some cases, several weeks) and expensive, so it is natural that managers may seek to reduce costs. The planning of an appropriate number of study meetings, the inclusion of expert team members, rather than staff who happen to be available, and the nomination of a trained and competent team leader, are all within the discretion of management. If these or other study parameters are compromised, the inevitable results are an inefficiently conducted study and ineffective hazard identification. Moreover, the study's poor returns are likely to be perceived by management as justifying their economies rather than as being caused by their decisions.

Such management thinking overlooks the fact that hazard identification is the foundation of all risk and safety analysis. Hazards not identified are not analysed or mitigated, so management economies at this stage of the process should only be taken in the light of clear understanding and should always be justified.

Another factor prejudicial to maximising the identification of hazards is the human tendency to perceive problems as unique when they are in fact examples of a wider class[9]. We tend to take the 'inside view' rather than the 'outside view'. Taking the latter would lead us to ask such questions as, 'What happened on the last occasion that we did something like this?' and 'Has anyone else done something like this and, if so, what happened?'. By taking the inside view we fail to consider, or even to recognise, relevant information. We neglect lessons that might be learned and experience that could be appealed to. We are likely to be overconfident in our plans (e.g. our system's design), to overemphasise their virtues, and to overlook their weaknesses.

A procedural way of neutralising the inside view is for a team rather than an individual to engage in hazard identification. However, the team needs to be carefully chosen[8]. Members must have different experience, responsibilities, and perspectives, for they need to complement each other. Beware the 'groupthink' of individuals with similar experience and outlook[10], for, ironically, they strengthen the conviction that their collective inside view is both correct and good.

A further technique that is often used for hazard identification is fault modes and effects analysis (FMEA), often called 'failure modes and effects analysis'. This seeks hazards by examining the effects of the failure of each component of a system. As the need for a team is not often emphasised, the method is often carried out by one person. However, an individual lacks the multiple viewpoints required in hazard identification, is subject to the inside view and an 'overconfidence bias', and is unlikely to carry out a thorough investigation. FMEA is also likely to miss hazards that result from the interactions of components rather than from the failure of the components themselves, and such hazards are frequent in modern complex systems, particularly those in which control is provided by software.

In summary, hazard identification is dependent on the subjective choice of techniques, and each technique not only carries its own propensity for error, but also is based on human judgement. If the adverse effects of subjectivity are to be reduced, it should be determined at the definition-of-scope stage which techniques are most appropriate, given the nature of the system to be studied. Then, in planning the study, the neutralisation of subjectivity should be considered. The range and types of hazards in even small enterprises or projects can be so large that no single method of identification is likely to uncover them all, and a combination of methods is most likely to be successful.


Whether the subject of risk analysis is a high-level policy or an industrial system, hazard identification can never be considered to be complete. Lowrance observed, 'We simply commit the sin of pride when we think we have been so smart as to have forestalled absolutely every possibility of failure.'[2] Indeed, the search for hazards should never cease. A hazard log should be maintained during the lives of safety-related projects and operational systems, and feedback from audits and interviews should be continuously screened for indications of hazards.

Further, formal hazard identification studies should be performed at several stages of the system's life[8], particularly when a new set of circumstances prevails and there is new information to be considered. Subjective decisions on when to carry out hazard identification can have a strong influence on the results of risk and safety analyses. Indeed, one of the greatest sources of error in risk analysis is the failure to identify hazards or the ways in which they occur. As Kletz points out, ever greater effort is expended on attempts to improve the accuracy of the estimates of the probabilities and consequences of hazards that have been identified while, in many cases, even greater hazards lie unseen[11].

## Hazard analysis

In engineering, risk is taken to be a function of an undesirable event's likelihood and potential consequences. Identified hazards must therefore be analysed for likelihood and consequence so that their risks can be estimated. This stage of risk analysis and the subjectivity involved in it will be the subject of a sequel to this article.

## Risk assessment (or evaluation)

When hazards have been identified and analysed, the risk-assessment stage is concerned with determining the tolerability of their risks. Typically, tolerability is assessed on the basis of both risk values and other factors, such as the benefits to be gained and the costs of reducing the risks. What is tolerable depends on the circumstances and on human values as well as on technological information, and, in the area of public policy, tolerability decisions are the subject of political processes. Comparing risks against benefits is hugely subjective, for a benefit to one person is anathema to another, just as an intolerable risk to one may be quite unacceptable to another.

Risk tolerability depends on how a risk is perceived, and risk perception differs greatly between people, the reasons being psychological, social, and cultural. For example, Slovic, Fischhoff and Lichtenstein conclude that perception is a function of many variables, such as whether the risk is voluntarily taken, who has control over it, and whether it has fearfully large consequences[12]. Wynne shows its relationship to trust in those with responsibility to manage the risk[5]. When risk-tolerability decisions are based only on likelihood and consequence, and imposed on the public, they are often resented and opposed.

## Discussion

The process of risk analysis involves subjective judgement at every stage. It is not an exact or objective process but a tool for arriving at approximate risk values so as to inform decision-making. Like all tools, it should be used within its limitations and with an understanding of its assumptions. It should not

be considered an end in itself, and its results should not provide the only basis on which decisions are made.

Judgement is required not only in carrying out risk analysis but also in using its results, which it would be wrong to portray as definitive. But even approximate estimates can be of considerable value—as long as we recognise that the numbers are likely to be crude—and having to focus on the risks is rewarded by a greater understanding of them.

Certain risks, for example those posed by genetically modified organisms, carry huge uncertainty, such that numeric values for probabilities and even for consequences are mostly speculative. In such cases, attempts to carry out quantitative hazard analysis are at best optimistic, and they can be misleading because numbers are often mistaken for accuracy. But the majority of risks subjected to analysis are concerned with the operation of equipment, the hazards involved in processes, and the safety of products. These, in most cases, are better understood. This does not mean that they don't carry uncertainty or that they are immune to subjectivity, but their analyses, whether quantitative or qualitative, are, in the main, effective in leading to risk reduction. Evidence for this exists in the vast number of industrial plants in operation, and products on the market, that are not perceived by the public as risk issues. However subjective it may be, risk analysis is a valuable tool, and modern safety standards demand that it be carried out. Indeed, UK law requires most businesses to produce documented risk analyses. But it could be improved.

The subjectivity identified above is a vulnerability, but it is also one of the principal strengths of the process. Identifying and analysing hazards and making decisions about risks demand human thought and human investigation. If the process were automated, it would not benefit from the human ability to probe and to take the situation as it is rather than as a programmer some time previously generalised it as being. But human delving means that something is always likely to be missed and some things may be wrongly judged. Thus, it is important for risk analysts to understand and allow for the subjective influences on the process. These should be addressed in training and in planning and managing the risk-analysis processes.

**Acknowledgements**

Versions of some parts of this paper were included in Redmill, F.: Subjectivity in Risk Analysis, Proceedings of Risk Analysis and Safety Management of Technical Systems, Gdansk, Poland, 25-27 June 2001.

**References**

1. United Kingdom Interdepartmental Liaison Group on Risk Assessment, Use of Risk Assessment within Government Departments, 1996
2. Lowrance, W.W.: The Nature of Risk, 1980, in Schwing, R.C. and Albers, W.A. Jr. (eds): Societal Risk Assessment—How Safe is Safe Enough?, Plenum Press, New York
3. Wharton, F.: Risk Management: Basic Concepts and General Principles, 1992, in Ansell, J. and Wharton, F.: Risk Analysis, Assessment and Management, John Wiley & Sons, Chichester
4. Kasper, R.G.: Perceptions of Risk and their Effects on Decision Making, 1980, in Schwing, R.C. and Albers, W.A. Jr. (eds): Societal Risk Assessment—How Safe is Safe Enough?, Plenum Press, New York
5. Wynne, B.: Technology, Risk, and Participation: On the Social Treatment of Uncertainty, 1980, in Conrad, J. (ed): Society, Technology, and Risk, New York, Academic Press
6. Wynne, B.: Rationality and Ritual: The Windscale Inquiry and Nuclear Decisions in Britain, 1982, Chalfont St Giles: British Society for the History of Science
7. Interim Defence Standard 00-58: HAZOP Studies on Systems Containing Programmable Electronics, Ministry of Defence, Glasgow, UK
8. Redmill, F., Chudleigh, M. and Catmur, J.: System Safety: HAZOP and System HAZOP, 1999, John Wiley & Sons, Chichester, UK
9. Kahneman, D. and Lovallo, D.: Timid Choices and Bold Forecasts. A Cognitive Perspective on Risk Taking, 1993, Management Science, 39, 17-31
10. Janis, I.L.: Victims of Groupthink, 1982. Second Edition, Houghton-Mifflin, Boston
11. Kletz, T.: HAZOP and HAZAN, 1999, Fourth edition, Institution of Chemical Engineers
12. Slovic, P., Fischhoff, B. and Lichtenstein, S.: Characterising Perceived Risk, 1985, in Kates, R.W., Hohenemser, C. and Kasperson, J.X. (eds): Perilous Progress: Managing the Hazards of Technology, Westview Press, Boulder



Felix Redmill, an IEE Fellow, is a consultant in risk management, project management and quality improvement. He is also Co-ordinator of the IEE Safety-Critical Systems Club. He can be contacted at Felix.Redmill@ncl.ac.uk.