THE SIGNIFICANCE TO RISK ANALYSIS OF RISKS POSED BY HUMANS[1]

by Felix Redmill
Redmill Consultancy
Email: Felix.Redmill@ncl.ac.uk

Humans - both operators and managers - contribute significantly to functional risk. Thus, even when risk analyses that omit human factors are good predictors of equipment failure, they are likely to be poor predictors of accidents. Engineering risk analysts could benefit from learning about and applying human reliability assessment methods, and risk analyses could benefit from addressing the risks posed by management, including senior management.

INTRODUCTION

Functional risks - risks caused by the operation of man-made systems - extend over a spectrum. At one end are those arising predominantly out of random events, such as the failure of electromechanical equipment. If appropriate historic data exist, it may be possible to derive the likelihood of similar failures in the future, with some confidence.

Moving along the scale, there is complex hardware, including modern electronics, in which systematic failures play a significant role. Systematic failures are those that would always be repeated (systematically) under the same conditions. They arise not from wear and tear but from specification and design faults.

Then there is software, in which all failures are systematic. If a systematic fault were discovered during testing, it would be corrected, but software is inherently complex, and the high number of logical paths through even relatively simple programs means that it is usually impossible to test exhaustively in cost-effective time. Moreover, even exhaustive testing against a specification does not trap the faults associated with unplanned or unexpected use of a system.

Further along the spectrum are human sources of risk. Human error is not random, but it may sometimes approximate to randomness. For example, exhaustion at the end of a long or arduous period of work, or during a night shift, may approximate to component wear-out. Human error can also be systematic, for example when a person who has been given the wrong training or information repeatedly makes the same mistake. But humans are also capricious and cause problems for numerous other reasons, for example by sabotage, acting on a whim, making decisions based on inadequate or incorrect information, and well-intentioned violation of rules. Thus, satisfactory modelling of human behaviour is not trivial or routine.

---

[1] Published in Engineering Management Journal, Vol. 12, No. 4, August 2002
and in Journal of System Safety, September-October 2005

Although functional risks pertain to operation, they need to be identified and analysed during the development of a system and reduced to a tolerable level in its design. Risk analysis has, within limits, proved effective in predicting equipment failure (and two previous papers (Redmill 2003, Redmill 2004) have addressed the limitations imposed by subjectivity in the risk-analysis process). However, most systems have human components, one being the operator whom engineering risk analysis has, until recently, tended to neglect. 'Human reliability assessment' (HRA) methods exist, but they remain largely in the domains of psychologists and ergonomists, and it is time for engineering risk analysts to understand and use them. The next section discusses the state of the HRA art. It also points to deficiencies that should lead to caution in the use of the techniques.

HRA methods mostly address the risks attached to the humans involved in system operation, but operators are not the only humans who influence functional safety. Managers, including senior managers, do so in a number of ways. At the lower levels, they do so in supervision, management style, task scheduling, and decision making. At more senior levels, they influence safety by their definition of strategies and policies and the culture that they nurture by design or default. Yet the risks posed by management are never (to this author's knowledge) included in risk analysis. This article points to the resulting shortcomings in analyses, argues for a new approach, and shows the scope for research into the subject.

HUMAN RELIABILITY ASSESSMENT AND ITS SHORTCOMINGS

Risk analysis forces analysts to identify and enquire into risks and their causes and consequences. This leads to an improved understanding of the systems posing the risks and the risks themselves, and lays the foundation for planning and taking action to improve safety. However, not addressing the risks posed by human operators means that risk analyses are necessarily underestimates - they may provide reasonable predictions of equipment failure but not of system failure. It also means that the risks posed by operators would not be mitigated to the extent that they would have been if the relevant risks had been understood. HRA methods are used in some industries, but, typically, engineers are not familiar with them. Although they are flawed, as discussed below, their use leads to an increased understanding of the human sources of risk and, thus, to more complete analyses and improved system safety.

During the 1970s and 1980s significant advances were made in the knowledge of human behaviour, the propensities for humans to err, and the ways in which they do. An early model to explain error mechanisms was Rasmussen's (1983) framework that proposed three types of error: skill-based, rule-based, and knowledge-based. This framework was built on by Reason (1990), who further defined the basic error types as being slips, lapses and mistakes. Kletz (2000) defines four error categories and points out that causes of an incident may include more than one of them:

- Mistakes - errors that occur because someone does not know what to do;
- Violations - errors resulting from someone who knows what to do deciding not to do it, usually for what appears a good reason;
- Mismatches - errors caused by a person's inability to carry out a task;
- Slips and lapses - errors due to lapses of attention.

In parallel with attempts to model the causes and mechanisms of human error,

techniques for human reliability assessment (HRA) were developed - see Caccuabue (1997) for a review. In the first place, the techniques approximate to hazard identification methods in that they provide ways of analysing operators' tasks and working environments and identifying likely causes of error. In the second place, they approximate to hazard analysis methods by attempting to attach probabilities to the identified hazards. This quantitative approach was not unnatural given that, at the time the techniques were developed, industrial risk analyses were mostly probabilistic and HRA techniques were intended to achieve similar aims of identifying and analysing risks. Although the hazard identification processes were qualitative and based largely on human judgement, the techniques were not seen as complete if they did not provide ways of attributing probabilities to error occurrences. For this reason, many HRA methods include databases of historic incident data from which numeric 'probabilities' of future events might be derived.

But probability theory is based on randomness, and, as randomness can, at best, offer only a partial explanation of human behaviour, its application to human error introduces assumptions that may not maintain in any given case. However, to be fair to the human factors practitioners who use the techniques, the numbers are often not taken in absolute terms and may be used only for prioritisation purposes. Engineers who try to use the techniques should be aware of the assumptions involved, of how the numbers are derived and used, and of the confidence that they can reasonably place in them.

As well as basing quantitative analysis on a qualitative and judgmental foundation, HRA techniques are weak because they do not embrace the most recent knowledge of human behaviour. The human factors experts have for a long time acknowledged this and called for the development of a new generation of techniques. For example, in the mid-1980s, Williams (1985) said that HRA methods were neither accurate nor easily usable by non-specialists and, 'The developers of human reliability assessment techniques have yet to demonstrate, in any comprehensive fashion, that their methods possess much conceptual, let alone, empirical validity.'

Swain (1988) said that all HRA models had serious limitations, that the task of calibrating the models had not been seriously addressed, and that they are often ill-founded relative to human behaviour. Dougherty (1990) agreed and asserted that 'inadequate HRA modelling can lead to increased risk or wasted risk management resources.' He called for second-generation methods to be developed and for advances in error psychology and cognitive science to be accommodated within the HRA framework. Later, Hollnagel (1996) complained of the obsolescence of the state of the HRA art. However, reliable second-generation methods have not yet replaced the first-generation methods.

HRA does not contribute fully to risk analysis, not only because of its deficiencies but also because in many industries it is not employed. There is a need for engineering risk analysts to become familiar with the techniques and to study human cognition and the models developed to explain human error. This is important with respect to modern systems at least as much as, and probably more than, to traditional electromechanical systems. In modern safety-critical systems, automation has increased rather than reduced the problems facing a human operator and the need to assess them. In the first place, even full automation would not eliminate human involvement in the system; it would merely transfer the critical responsibilities from the operator to the designer. Then, partial automation often

makes the operator's role supervisory, usually with reduced information. Not only is supervision a task not conducive to humans, but, due to less training and less hands-on experience, operators become de-skilled but are still expected to resume control and take time-critical decisions when the automated system fails - often in an emergency. The likelihood of human error may therefore be increased.

Though tricky, human reliability assessment needs to be carried out. Yet, it is omitted from many, if not most, risk analyses, and HRA techniques are largely unknown to engineering risk analysts. Further, engineers have little guidance on the subject, for safety standards do not advise on it. The influential international safety standard, IEC 61508 (IEC 2000) addresses hardware and software functional safety in great detail, but offers no advice on human factors. HRA methods are in some respects flawed, but if used with care, they facilitate a significant but overlooked aspect of risk analysis.

Engineers in safety-critical fields now need to get to grips with the important and expanding subject of 'human factors'. They also need to bring human factors experts into systems-engineering teams so as to incorporate human influences into both system design and risk analysis. If they fail to do so, risk analyses will continue to omit what in many cases are the greatest hazards.

HOW RISKY IS MANAGEMENT?

Notwithstanding the limitations of HRA techniques, their application, when it occurs, is almost invariably confined to the humans directly concerned with equipment and whose errors may be the final causes of accidents. Equipment operators are the obvious human components of systems, but they are far from being the sole human causes of accidents. It is now recognised that the policies and strategies defined by senior management, and the cultures created (by design or default) and engendered by them, predispose accidents to occur or not to occur, and that the final triggering event is often merely the activation of an 'accident waiting to happen'. In the inquiries into numerous major accidents, including the Chernobyl nuclear explosion, the sinking of the Herald of Free Enterprise, the *Challenger* space shuttle explosion, and the Piper Alpha oil rig fire, senior management failure was concluded to be a primary cause.

Kletz (2000) distinguishes management failure from human error, and says that it occurs because senior managers do not realise that they could do more to prevent accidents. He contrasts management's perception that they have no need to get involved in the detail of safety issues with their close attention to output, costs, and even product quality. He also contrasts the effort expended on investigating three generic accident causes with their actual importance (see Figure 1) to show the distortion in senior management's consideration of their own failures.

Yet, it is unheard of for a risk analyst to address the influence of senior management on functional risk, and this exclusion of a major accident cause from risk analysis must lead to optimistic results - contrary to the aim of risk analysis. Not is management risk addressed by HRA.

In her examination of the origins of the *Challenger* space shuttle disaster in 1986, Vaughan (1996) points to mistake and disaster being 'socially organised and

systematically produced by social structures'. She says that the cause of the disaster was 'a mistake embedded in the banality of organisational life' and she shows how 'deviance in organisations is transformed into acceptable behaviour'. The features of organisational life amount to the culture of the organisation, and a principal role of senior management is to engender and nurture a culture that ensures that such transformations do not take place. It would be simplistic to say that the occurrence of such transformations is clear evidence of management's failure, for industrial accidents are usually the result of not one but multiple failures. But it is reasonable that they should raise questions about management's performance with regard to safety - as indicated in many accident inquiries, including those mentioned above.

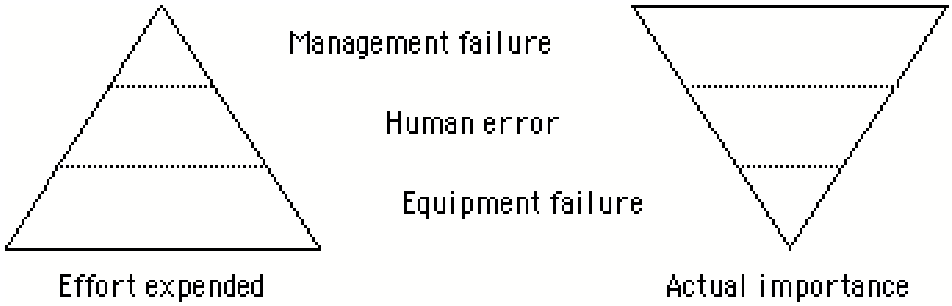

Figure 1: The effort expended on different causes of accidents and their actual importance

In his investigation of the *Challenger* disaster, Feynman (1989) found that engineers at the National Aeronautics and Space Administration (NASA) considered the chance of a shuttle failure to be about 1 in 200 launches and, at best, 1 in 1000. But he found that NASA management took the figure to be 1 in 100,000 launches - which, as Feynman pointed out, would mean that a shuttle could be launched every day with an average of almost 300 years between accidents. The engineers were the experts, and historical data suggested that their estimate was accurate, but organisational decision-making was carried out as though management's estimate was correct.

The development of a safety culture, and, indeed, of appropriate processes for reducing risks, depends on the ability and willingness of humans - and, in particular, management - to learn lessons from past mistakes and incidents, and to apply them. A significant management error, therefore, is the failure to learn and apply the lessons of past mishaps to prevent future accidents. Kletz (1993) explains this error, saying, 'It might seem to an outsider that industrial accidents occur because we do not know how to prevent them. In fact, they occur because we do not use the knowledge that is available.' This is almost inevitable if management leaves the learning of lessons to lower-level individuals rather than building them into methods of working.

Risk analysts go to great effort and expense to determine quantitative estimates of the likelihood of the final triggers of hazardous events - mainly equipment failures. Sometimes they assess operator causes. But they ignore the predisposing factors created by management, and in many cases these pose significant risks. By ignoring management issues, and, in particular, senior management issues, risk analyses are predisposed to be weaker predictors of accidents than of equipment failure.

THE NEED FOR RESEARCH

There is a need for research into how management risks may be modelled, estimated and predicted. But with risk analysis being a relatively well established process, why should it require research to improve it rather than merely the introduction of improved procedures? Because working-level engineers and risk analysts are not positioned (and often not competent) to analyse the risks introduced by senior management. In general, they are not sufficiently familiar with the sources of the risks - company policy, strategic plans, management style, and organisational culture - to be able to carry out hazard identification and analysis studies on them. Indeed, they are unlikely even to have access to some of the requisite information. Investigation of the risks under discussion would not be within the ambit of someone carrying out risk analysis in the traditional way. Research is necessary to develop and test methods of identifying management hazards, determining the ways in which they might lead to disasters, and estimating their likelihood of doing so.

Methods also need to be developed for reducing management risk. In the first place, safety needs to be a permanent item on the Boardroom agenda. In some cases the requirement may be for environmental policy, in others the crucial issue might be the safety of workers, or the public, or the users of particular products. In the second place, Boardroom audits should be introduced to ensure that safety issues are addressed invariably and fully. Then Boardroom and company audits could be correlated to monitor the manner in which functional risk is addressed by senior management. For this, auditable issues need to be defined, and these should include the ways in which safety is addressed in company policies and strategies and the appropriateness of these to the organisation's safety issues.

Further, because there is often a lack of senior management awareness of whether or how their policies and strategies are implemented, audits need also to examine the ways in which senior management ensure and monitor their implementation. The minutes of board meetings could be audited to ensure that these topics are properly addressed, and company audits could investigate the correlation of actuality with the board's minutes.

A high-level risk analyst would then bring the boardroom and company audits together with 'traditional' risk analyses to produce an improved analysis that would be a better predictor of risks and more in keeping with modern safety requirements.

At the same time, research might usefully investigate the relationships between safety culture and such issues as high-level policy, strategy, and management style, with findings leading to further items that could be subject to semi-objective audits.

If large technical changes were made to the existing risk-analysis process, they might improve it marginally. But smaller 'soft' changes, which bring the risks posed by senior management into the analysis and introduce an ability to identify organisational risk, could bring about much greater improvements to safety.

The above are merely initial thoughts on research topics. However, in recent years there has been an increase in the attention paid to ‘corporate governance’. In promoting this, the Institute of Chartered Accountants in England and Wales produced a code on internal control, and guidelines on conforming to it (ICAEW

1999). These call on companies to carry out analyses of all their significant risks, and regularly to review the effectiveness of their internal controls, including risk management. Further, the London Stock Exchange has recommended that its members explain in their annual reports how they have applied these and other principles.

This advance has the potential to reduce the risks of accidents caused by management failure, but it does not explain how such risks can be included in system risk analyses. There is still a need for research into this, as suggested above, and into the motivators and de-motivators for organisational learning.

DISCUSSION

Traditionally, in addressing system safety, engineering risk analysts have tended to neglect the risks posed by humans. This provides optimistic results, for humans are major contributors to functional risk. Further, because the proliferation of safety-related systems means that risk analysis is carried out in most industry sectors, it is a widespread problem. It is therefore time for risk analysts, and engineers in general, to develop an understanding of human cognition and behaviour, and of HRA techniques, and to address human factors in functional risk analyses. Engineering and risk-analysis syllabuses need to be reviewed to facilitate this.

As the available HRA techniques suffer from a number of flaws, engineers need to understand their assumptions so as to use them beneficially within their limitations. Concurrently, research is required, in the fields of both engineering and human factors, to develop improved methods that more closely reflect the understanding of human behaviour arrived at over the last two decades. Research should also seek user-friendly ways of integrating HRA into system risk analyses.

It is also time for the recognition of the importance of a multidisciplinary approach in safety engineering and management. There is an urgent need to improve safety and reliability by bringing human factors experts into the overall process of systems engineering, particularly in requirements engineering and design. At the same time, engineers need to develop their knowledge of human cognition and ergonomics so as to facilitate communication with, and understanding of, their human-factors team mates.

Engineers must also recognise that assessing operator error goes only part of the way to addressing the human influence on functional risk. The risks posed by operators are often less significant than those introduced by management via policy, strategy, management style, organisational issues, culture, and decision-making. Ways of assessing management risks, and including the assessments in functional risk analyses, are required, and thoughts on first steps towards this are offered in this paper.

The risks posed by operators and managers may often outweigh those posed by hardware and software. Thus, if risk analysis is to meet the requirements of the modern technological environment, it must be developed to include the risks posed by both of these human contributors. Doing this offers scope for research in the interesting field created by the overlap of engineering and psychology, and also for a review of industrial procedures.

REFERENCES

Cacciabue C (1997). Human Reliability Assessment: Methods and Techniques. In Redmill F and Rajan J (eds): *Human Factors in Safety-critical Systems*. London, Butterworth-Heinemann

Dougherty E M Jr (1990). Human Reliability Analysis - where shouldst thou turn? *Reliability Engineering and System Safety*, 29, 283-299

Feynman R P (1989). *What Do You Care What Other People Think?* Unwin Hyman, UK

Hollnagel E (1996). Reliability Analysis and Operator Modelling. *Reliability Engineering and System Safety*, 52, 327-337

ICAEW (1999). Internal Control: Guidance for Directors on the Combined Code. *The Institute of Chartered Accountants in England and Wales*, London

IEC (2000). *International Standard IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Systems*. International Electrotechnical Commission, Geneva

Kletz T (1993). *Lessons from Disasters*. Institution of Chemical Engineers, London

Kletz T (2000). *An Engineer's View of Human Error.* Third edition, Institution of Chemical Engineers, London

Rasmussen J (1983). Skills, Rules, Knowledge: Signals, Signs and Symbols and Other Distinctions in Human Performance Models. *IEEE Transactions on Systems, Man and Cybernetics*, SMC-13, 3, 257-266

Reason J (1990). *Human Error*. Cambridge University Press

Redmill F (2003). Risk Analysis - A Subjective Process. *Journal of System Safety*, Vol. 39, No. 2, 1st Quarter 2003

Redmill F (2004). Subjectivity in Hazard Analysis. *Journal of System Safety*, Vol. 40, No. 1, January-February 2004

Swain A D (1988). Adapting Risk Analysis to the Needs of Risk Management. Paper presented at *World Bank Workshop of Risk Management and Safety Control*, Washington D.C.

Vaughan D (1996). *The Challenger Launch Decision*. University of Chicago Press, Chicago

Williams, J. C. (1985). Validation of Human Reliability Assessment Techniques. *Reliability Engineering*, 1985, 11, 149-162