Risk assessment tools: Good servants, poor masters

Harvey Dearden discusses the business dangers of fearing the worst in risk assessments

RISK assessment tools should come with a health warning: "uncritical use may seriously damage your business". Worst-case assumptions may appear prudent, but their undiscriminating use may seriously undermine the value of a risk assessment in identifying the appropriate allocation of resources. There are a variety of approaches that may be adopted in undertaking risk assessments in support of the development of a safety case or safety integrity level (SIL) determination. There is a spectrum of possibilities ranging from the purely qualitative, through semi-quantitative to the fully quantified. In assessing risk, the UK's Health and Safety Executive (HSE) employs the concept of proportionality – ie risk assessments and adopted risk reduction measures are required to be proportionate to the risk. In essence, the greater the risk:

- the greater the required degree of rigour in the risk assessment and the demonstration of ALARP; and
- the more a duty holder would be expected to pay to reduce those risks.

A risk may be characterised as having high proportionality if it is assessed as approaching the intolerable region of the HSE's risk triangle, which categorises risk as being "broadly acceptable", "tolerable if ALARP" (as low as reasonably practicable), and "intolerable".

Proportionality should not be confused with proportion factor, which is the ratio of the cost of preventing a fatality (CPF) and the value of preventing a fatality (VPF) and which may be used in assessing whether any further expenditure on incremental risk reduction would be grossly disproportionate as a test of whether a risk was ALARP.

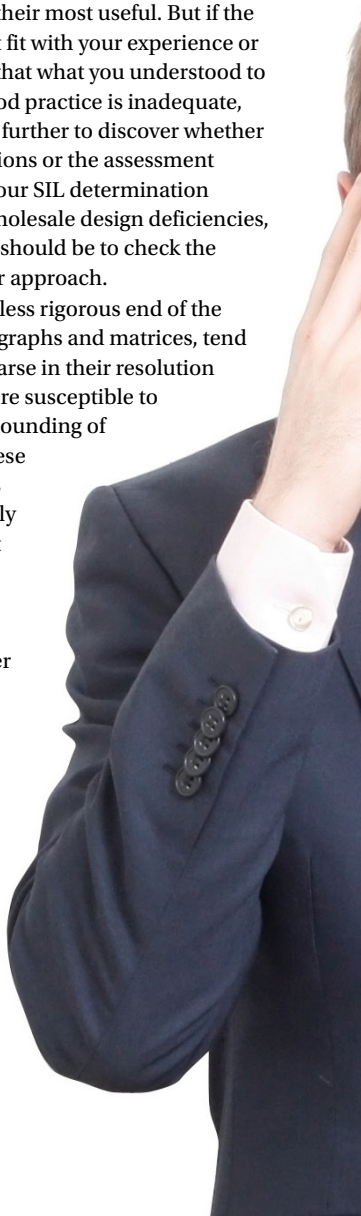
inevitable uncertainties

Some of the available risk assessment techniques are highly refined, but this should not blind us to the inevitable uncertainties in the results. A rigorous process will not compensate for uncertain data, and any quest for absolute accuracy is doomed. A particular problem is the compounding of conservatism: a succession of worst-case assumptions that is thought to represent an upper bound to risk will quickly generate gross distortion of the overall assessment. It may well seem prudent to err on the side of caution, but do this at successive points and your analysis may well be one or more orders of magnitude from a true estimate. It might be argued that the distortion is safe but if it causes a misdirection of resources or an unwarranted elaboration of provisions which are more difficult to manage/maintain, the result may well be an overall net loss of safety in practice.

A wrongheaded and naïve approach is to perform a risk assessment and unquestioningly accept the outcome as definitive. The outcome should always be critically reviewed to see if it appears sensible. It may be that the assessment reveals hitherto unrecognised levels of risk or identifies an element as being of more significance than was previously understood. It is perhaps when revealing any such anomalies that these tools are at their most useful. But if the outcome does not fit with your experience or seems to suggest that what you understood to be established good practice is inadequate, you should probe further to discover whether it is your expectations or the assessment that is flawed. If your SIL determination process reveals wholesale design deficiencies, your first thought should be to check the calibration of your approach.

The tools at the less rigorous end of the spectrum, eg risk graphs and matrices, tend to be relatively coarse in their resolution of risk and are more susceptible to inadvertent compounding of conservatism. These less rigorous tools might be effectively deployed as a first pass filter with apparently higher risk scenarios parked for a higher resolution and higher rigour assessment.

> *"if the actual probability does indeed approach zero, the assessment of the risk associated with an explosion will have been inflated by a factor approaching infinity!"*

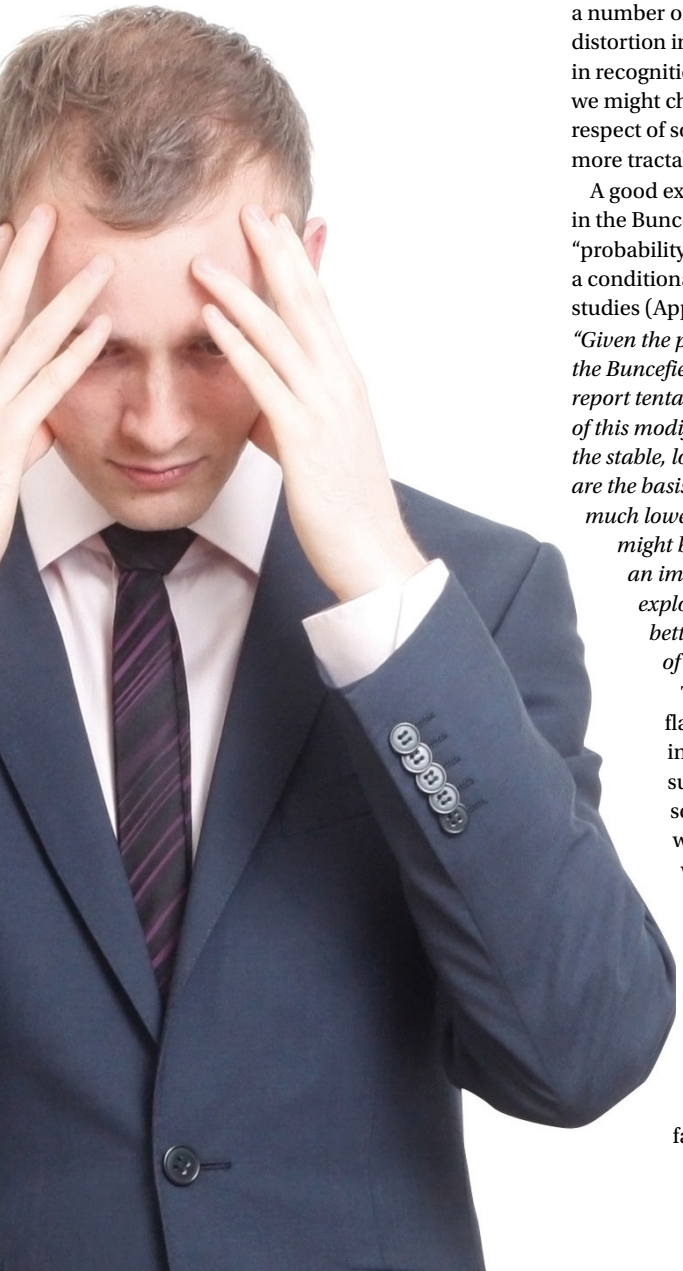


The key point is that risk assessment should be performed to validate your judgement (which should itself be suitably informed by training, experience, knowledge of good practice and an understanding of pertinent mechanisms) rather than to attempt to directly and definitively establish the true level of risk.

It was in recognition of this that the original *Code of professional conduct for engineers and risk issues*, as published by the Engineering Council UK in 1997 said: *"Uncertainty is a feature of many aspects of risk management. Be aware of this, and use risk assessment methods as an aid to judgement, not as a substitute for it."*

a judgement call

It may be that after critical probing to find the reason for any discrepancy between your expectation and the assessment, you may be obliged to recalibrate your judgement. Embrace the opportunity, this is quality CPD. The new risks must then be addressed in an appropriate, responsible manner.



Clearly what is not acceptable is to cynically manipulate the risk assessment to remove any embarrassment or inconvenience.

On the other hand, your critical review may find that the assessment is flawed in some way – perhaps through inadvertent compounding of conservatism or some critical omission; perhaps a missing conditional modifier or enabling event; or some circumstance that should be factored in to the analysis to qualify the true hazard potential. For example, a flammable release risk should be qualified on the basis of the likely size of the release; the presence and vulnerability of people; the likelihood of a source of ignition; the likelihood of detection and effective intervention; and the likelihood of the absence of a good stiff breeze etc.

Very often it will be self evident that the probability of a given circumstance will be less than 100%, but there may be no ready means of evaluating how much less. The default position is therefore to conservatively assume a probability of 100% – not unreasonable in itself, but if repeated a number of times we may suffer gross distortion in our final estimate. It may be that in recognition of this 'default' conservatism we might choose *not* to be conservative in respect of some other provision which is more tractable in estimation.

A good example is the guidance given in the Buncefield report[1] in terms of the "probability of explosion after ignition" as a conditional modifier to be used in LOPA studies (Appendix 2, clause 141):

"Given the present state of knowledge about the Buncefield explosion mechanism this report tentatively proposes that the value of this modifier should be taken as unity in the stable, low windspeed, conditions that are the basis of this hazardous scenario. A much lower, and possibly zero, probability might be appropriate. It's possible that an improved understanding of the explosion mechanism may allow a better basis for determining the value of this factor in the future."

The explosive (as distinct from flash fire) nature of the Buncefield incident was something of a surprise; the implication would seem to be that the circumstances were unlikely, otherwise there would have been no surprise; the phenomenon would have been well known and the possibility recognised.

If the actual probability does indeed approach zero, the assessment of the risk associated with an explosion will have been inflated by a factor approaching infinity!

relative risk

This highlights the need to be wary of accepting risk assessment quantification as providing any measure of absolute risk. These tools are typically more useful in providing a measure of relative risk and providing a means of comparison. This is of particular significance if you are to perform any cost benefit analysis, since this requires that you postulate before and after levels of risk and the corresponding cost. Expenditure typically secures an additional risk reduction factor (rather than an absolute amount of reduction) and the apparent benefit will therefore vary with the identified level of risk 'before'. There is more benefit from a factor-ten reduction in the annual probability of a hazardous event from 10^{-2} to 10^{-3} than there is from 10^{-3} to 10^{-4}.

It is all very well taking the anti-Panglossian[2] view of "all for the worst in the worst of all possible worlds", but we need to be smarter than that when deciding how to allocate limited resources. If there are a number of provisions in the analysis that are known to be conservative by indefinite amounts, it may be appropriate to aggregate these and assign a factor to their combined influence in order to counter the distortion that would otherwise arise with compounding conservatism.

You may find that an iterative development of both your understanding and the assessment is required until your increasingly-educated expectations converge with the increasingly-refined analysis. Far from being a 'massaging' of the numbers, this is the proper and responsible approach of the professional engineer. There is a world of difference between modifying a risk assessment because it is not judged sensible and because it does not fit the budget.

If it comes to a debate with the HSE about a risk assessment or safety case, remember that their inspectors will approach these questions from a distinct perspective. Understandably, this is unlikely to embrace your wider business concerns and resource constraints. It is for the duty holder to make a robust case that also recognises these issues. The HSE may well urge you to conservatism, which undoubtedly has its place in a prudent and responsible approach, but if you find this to be leading to unwarranted distortion you should stand ready to defend your judgement. **tce**

Harvey Dearden (htdearden@tdsl.org.uk) is technical principal and managing director of Time Domain Solutions

1. *Safety and environmental standards for fuel storage sites,* Final report, HSE 2009
2. Pangloss being the character in Voltaire's *Candide* who continually asserts that "all is for the best in the best of all possible worlds"