

The management of system risk: Safety and environmental risk in engineering and transport

Dr Chris Elliott FEng, Pitchill Consulting Ltd

What is risk?

Ever since a caveman decided to bring fire into the cave, we've been living with risk. That caveman knew that fire was dangerous, but he decided that the benefits of a warm home and cooked food more than compensated for the risk that his home might catch fire. Since then, it is hard to think of any beneficial innovation, social or technical, that didn't bring with it the possibility of harm.

If society were to forbid any activity that might cause harm, we would lose the benefit of electricity, medicine and much else, including all sports and entertainment. But equally we cannot allow total freedom to do anything, whatever and whomever it might harm. Society has to find a way of deciding what is acceptable and managing it to prevent catastrophe.

It is helpful to distinguish hazard (anything that can cause harm) and risk (the chance that a hazard will cause harm, and the extent of that harm). The objective is then to manage the risk, not to eliminate the hazard. The caveman knew that fire was a hazard, but he realised that, if he kept it in the hearth and made his children stand back, the risk was low enough to be worth taking in order to have a warm cave.

That argument is enough when the person taking the decision will suffer the harm if the hazard materialises and will receive the benefits if it does not. A serious ethical challenge arises where individuals cannot decide for themselves whether to take a risk, either because they do not have sufficient information or because they do not have sufficient control. This is made even harder when the benefits and potential harm do not fall to the same people, especially if the benefits occur now and the potential harm is to future generations.

Many engineering and transport risks are like that – I want to explore how a responsible and ethical engineer meet social demands when he knows, at least statistically, that what he is doing will injure or kill people or harm the environment.

The legal and ethical duty

There are two principles:

- *risk is the responsibility of the person who creates it* - "...it shall be the duty of every employer...", Health and Safety at Work Act 1974, Polluter Pays Principle, Art 130R(2) EC Treaty
- *risk cannot be eliminated* - "As Low As is Reasonably Practicable" (ALARP), "Best Available Technology Not Entailing Excessive Cost" (BATNEEC).

But what does "reasonable" mean? It's a common word in our law. You may use *reasonable* force in self-defence or to evict a trespasser, and you are not negligent if you use *reasonable* skill. What is reasonable at any time is what society believes to be reasonable. The Courts try to reflect this, taking into account the circumstances under which you acted, such as in haste or with time for reflection) and whether your activity was recognised as useful, such as providing a transport service or rushing to put out a fire. But there are very few rulings by Courts that provide much guidance on where to draw the line between reasonable and unreasonable.

One way of expressing society's view of what is reasonable is to estimate how much it is willing to pay to avoid a risk. When deciding whether to adopt a safety measure or to permit an activity, we work out how much it will cost or save and how much risk it will cause or remove. We can then estimate the cost-effectiveness – how much safety we will buy per pound that we spend. The National Institute for Clinical Excellence does this for medical treatments and ranks them in order of cost-effectiveness. The budget for the NHS then determines how far we can go down this list before the money runs out. The Department for Transport publishes an annual figure for the Value of Preventing a Fatality (VPF). We can compare this with the cost of a safety measure in terms of Cost per Fatality Avoided (CPF).

This hard-nosed economic approach puts an important demand on engineers. We have no right to plead that a safety measure is not cost-effective unless we are confident that our costs are under control. We should not rule out a safety measure as too expensive if its high cost is a result of our incompetence.

But we don't let this hard-nosed economic approach be the only thing that determines what we will permit or forbid. We recognise that society cares more about some kinds of risk than others, and that we must reflect what public opinion demands. That then begs the question – how do we determine what public opinion demands?

Where do we find representative public opinion? We certainly do not find it in the media. Even the broadsheet newspapers present at best an incomplete view of risk, and in many cases they actively distort the truth to print an eye-catching story. Railways have been grossly misrepresented – the number of fatal train accidents and the number of passengers killed were both fewer after privatisation than before, but few people are aware of that. The nuclear power industry struggles against a perception that it is more dangerous than “safe” coal or gas power, and parents wrestle with the belief that paedophiles lurk around every corner.

The result of this misreporting is that people simultaneously hold two views. Research in the transport and food industries has shown that they believe that the train or food is safe enough and nothing more should be spent on safety, but that it is outrageous that accidents are allowed to occur and the Directors of the companies responsible should be punished. What should the responsible engineer do now? Should he lower an already low risk because people are outraged, taking resources away from other more serious causes of harm, or should he deal directly with the feeling of outrage? The second approach brings him into the territory of Corporate Social Responsibility.

The traditional view of social responsibility was that people vote for Parliament and Parliament, through legislation and Ministerial oversight, reflects their views. That is no longer enough. Civil society embodies a wide range of interest, pressure groups and extra-parliamentary political processes and the responsible engineer has to engage with all of them to gain and retain his informal licence to operate. If he does that, he can do what society demands, which is to provide the proper balance of safety, cost and performance

Back to systems

My definition of a system is “*a set of parts that, when brought together, exhibit properties that were not present in the parts alone*”. Those properties, including risk or safety, cannot be managed by managing the parts alone; you have to manage them as a system. This raises two important risk management issues: how to apportion risk between the parts and what about risk that emerges from the interactions of the parts?

We can apportion risk – the total risk arising from a system can be shared out, so that each part has to present no more than its share of the total. An environmental example is the use of cadmium in NiCd

batteries. We should all like to reduce the risk of exposure to heavy metals, such as cadmium, and one of its sources is the manufacture, use and disposal of NiCd batteries. However, when we share out the risk to people from cadmium, we find that Europe receives around 219 tonnes per year from natural sources, around 415 tonnes from other industrial and agricultural uses and around 2.5 tonnes from NiCd batteries. Their share of the risk is small and they have unique advantages over other technologies for use in power tools and at low temperatures. The risk reduction from banning NiCd batteries would be more than outweighed by their benefits, especially when there is a growing recycling campaign. Also, the law of unintended consequences kicks in – the cadmium that they use is a by-product of producing zinc and would be sent to landfill if not used in batteries. Conclusion: the residual risk arising from NiCd batteries if everything else were eliminated is too small to justify banning them.

Similar logic applies to safety risks. Submarines have an escape tower that allows the crew to escape if the submarine is disabled at depths up to 200m. There are many possible ways to reduce the risk to submariners, one of which is to allow escape from greater depth. However, a risk-based analysis shows that less than 1% of the ocean has a depth between 200m and the hull crush depth, and also that most accidents are caused by collisions which are most common near ports and therefore relatively shallow. The fraction of the total risk that can be apportioned to sinking in greater than 200m is tiny, and there are other more cost-effective ways to invest to reduce risk.

In both of those cases, a proper risk-based process led to the conclusion that it is not necessary to take any further action to mitigate the risk. The hazard is still there, but the risk is properly controlled. That sort of process is the most robust defence against knee-jerk reactions and misrepresentation.

But what happens when the risk arises solely from the interaction of the parts of the system. You can't then apportion the risk to each part – it makes no more sense than to try to describe the sound of one hand clapping. Instead, we try to define what each part will do rigorously so that their interactions are wholly predictable. In practice, of course, specifications are rarely perfect (especially when there's software involved). This is the area where engineers' approaches to risk are weakest, and where caution and hazard management may take precedence over risk assessment.

System risk is compounded when the different parts of the system are under different ownership or management, such as in transport. The fundamental principal of holding the risk's creator responsible means nothing, because no one person did create it. If the interface specification is not perfect, we may find that some risk has two owners, who may not agree on how to manage it, and there may be orphan risk with no owner. Who then is responsible? Interestingly, Lord Robens recognised this in his report that led to the Health and Safety at Work Act. He never envisaged that regime being applied to a transport system.

In conclusion

We have a well-defined approach to managing safety and environmental risks, but two challenges remain. The first is to find a clearer way to judge what society demands of duty holders, in a climate of rational debate. The second concerns fragmented systems, where concepts like duty holding and the Polluter Pays Principle start to break down. Then the companies that make up an industry must work together to find solutions that address the whole problem and produce the optimum outcome for the industry as a whole.

Safety-critical industries can rise to these challenges – they do not want the alternative of more State intervention – but they need a constructive dialogue with Government, Parliament, Regulators and wider civil society.