



Safety in engineered systems

A discussion at The Royal Academy of Engineering

1. Introduction and recommendations
2. The need for a professional approach to the safety of engineered systems: Charles Haddon-Cave QC
3. An industrial view on institutional support for safety engineering: Keith Williams CEng, Group MD Altran Praxis
4. Coordination across industrial sectors: Dr Chris Elliott FREng, Pitchill Consulting Ltd
5. View from the safety specialists: Allan Bain CEng, Development Director, Safety and Reliability Society
6. View from the profession: Jon Prichard, CEO, the Engineering Council

1. Introduction and recommendations

Introduction

This report outlines the views of a meeting held at The Royal Academy of Engineering in response to Recommendation 28.4 of the Haddon-Cave Report (the Nimrod review). The recommendation stated: *A single professional body should be formed for safety experts to set professional and ethical standards, accredit members and disseminate best practice. Currently, there are a number of different professional bodies which provide some learned society facilities for those with some expertise in the safety field. There is a need, however, for a single professional body to provide focus, rigour and a centre of excellence.*

In the light of this review, a meeting was held at The Royal Academy of Engineering involving a range of professionals from across the engineering profession, industry and others with an interest in safety and safety systems. This report summarises the discussion on the day. It should be noted that it does not represent the policy position of the Academy, which, with partners in the engineering profession, will continue to explore the issues highlighted in the report.

Scope of discussion

Most engineers would agree that safety is one of the primary – if not the primary – concern of professional engineers when designing or assessing systems and products. However, there is a continuing need to ensure that engineers' skills in managing risks are both developed and used to ensure the safety of engineered systems. This need was highlighted in the recommendations of the Haddon-Cave review of the Nimrod crash.

The meeting addressed the following issues:

- Does the engineering profession require a new body to uphold standards of safety for engineered systems?
- Should safety be integrated into all other aspects of professional engineering practice?

- Can the existing engineering institutions and safety bodies cover this task, and what do they need to do to help prevent further accidents like the Nimrod crash?

Specifically, the meeting considered whether every professional engineering institution ensures that the proper management of safety is a core competence within its professional formation; and how all professional engineering institutions and other relevant bodies can cooperate to share experiences and transferable lessons and to support industry.

The meeting was first presented with a range of arguments supporting the implementation of Haddon-Cave Recommendation 28.4, with the intention of increasing cooperation and sharing of experiences by existing institutions rather than creation of a new professional body. There then followed a wide-ranging discussion which identified the need for safety to be understood across sectors and disciplines, the need for an holistic and unified approach, and the importance of recognising that safety is about people, not about procedures.

Views of the meeting

The consensus view of the meeting was that:

- More needs to be done to advance the management of safety in complex engineered systems and to ensure its understanding by all engineers working in all domains, across the UK.
- The professional engineering institutions should take coordinated action to ensure that an understanding of the trade-offs and judgements that determine the acceptable level of safety is part of every engineer's professional formation.
- Some engineers may choose to specialise in this field, for example when dealing with very complex engineered systems, in order to contribute specific expertise to the team responsible for delivering a system.
- The Royal Academy of Engineering should act as a 'fulcrum', providing a neutral platform on which the professional engineering institutions may share and align their initiatives and should extend the scope of its interactions to bodies charged with developing management and leadership, such as the Institute of Directors.

2. The need for a professional approach to the safety of engineered systems: Charles Haddon-Cave QC

The Haddon-Cave review of the Nimrod crash revealed a number of lessons for safety in engineering. Key to these lessons was the importance of engineering valuing its core technical skills and values; the importance of engineers recognising their responsibility; and the need for engineers to abandon the 'comfort blanket of procedure'.

Engineering institutions have made safety a core value. This attitude should spread throughout the profession, and the institutions have the key role in ensuring that this value is maintained. The following is a summary of the core lessons from the Nimrod crash in the form of seven principles, which could be used by engineering institutions and professionals to further promote safety as a core value.

1. Beware of making assumptions: assumptions are the root of mistakes, and questions are the antidotes to assumptions.
2. Value engineers and engineering, including those at the technician level.
3. Avoid 'plain sailing' and dig below the surface to find out what matters.
4. Avoid 'paper safety', i.e., an over-reliance on written safety cases. Safety is about people, not procedure.
5. Do not be risk averse, be risk sensible.

6. Outsourcing can be a threat to safety – need visibility and control to manage risk.
7. Avoid the dangers of PowerPoint engineering. This leads to watching rather than thinking.

3. An industrial view on institutional support for safety engineering: Keith Williams CEng, Group MD Altran Praxis

There is much to commend the UK's approach to safety. Many international companies regard the UK as a benchmark in terms of safety culture, standards development, delivery and regulatory expectation and enforcement.

The UK has delivered some exceptionally complex and safety-critical systems with excellent safety records over decades in many industries. Many key developments in the safety of engineered systems have emerged from the UK and there is much for UK industry to be proud of. These positive aspects must not be lost.

However, there are also some significant issues:

- Currently there is no means to develop or measure our engineers' safety competence in an industrially recognised manner. Compare this with Workplace Safety, where there exist widely recognised qualifications gained in a competitive CPD environment.
- In the area of complex systems, there are wasteful safety and certification processes and cultures, which add little to safety and add much to cost and waste a lot of paper.
- There is often a lack of focus on safety by design and operation, as opposed to safety demonstration by process and compliance.
- There are challenges to winning safety-critical work in an international context as a result of UK safety approaches and pricing.
- There is no forum for business-focused discussion on how effectively to implement safe systems while maintaining competitiveness. If the UK does not implement such systems, other nations will.
- It is very difficult to recruit engineers with the right competence and, crucially, the right engineering and operations-centred approach to safety.
- There is a lack of industrialised innovation in the achievement and demonstration of safety.
- There are periodic well-meaning initiatives within institutions, led by motivated individuals, but these are often in silos, lacking executive-level support and business involvement.
- Some of the safety-focused institutions are relatively small and need support.
- The UK has no joined-up engineering voice on these topics, despite the issues being common and faced by all branches of engineering. There are some differences, but these are subtle and not significant.

So, although there is much to commend in the UK's safety approaches, there are some issues to be addressed.

Given the importance of these issues, ethically and competitively, for the UK, and given the crucial role the engineering institutions need to play, it is very important that they lead the way and cooperate as one on safety to support UK engineering. These issues need wisdom and leadership before they can be resolved. The institutions are ideally placed to provide both this wisdom and leadership, and to highlight the following key issues:

- The need to improve engineers' CPD in the area of safety.

- The need to improve the effectiveness of engineered safety with the focus on design and operations-centred approaches to safety.
- The importance of maintaining UK competitiveness – ensuring the UK can build safety-critical systems in a competitive international market and encouraging UK innovation in this field.
- The provision of a common engineering voice on safety.

4. Coordination across industrial sectors: Dr Chris Elliott FEng, Pitchill Consulting Ltd

Engineering, like law, has to deal with grey areas – right and wrong are difficult; in both professions what is right depends on the quality of your analysis and arguments.

Conducting the trade-offs at the heart of engineering is subject to uncertainty and risk. Nothing is completely safe. We may have to accept the existence of a hazard (ISO definition ‘potential source of harm’) but we seek to minimise the risk (ISO definition ‘combination of the probability of occurrence of harm and the severity of that harm’). So we reach the ISO definition of safety – ‘freedom from unacceptable risks’ – which begs the question of what is acceptable and takes us back to law.

Engineers have to make trade-offs against conflicting requirements, and this concept of what is reasonable will be key in making such trade-offs. It follows that safety can never be the sole concern of professional engineers; it is one of the concerns that has to be balanced with others. This is particularly hard when those who are making the trade-offs – the engineers – are not those exposed to the risks.

Risk does not respect national, professional or sectorial boundaries. For example, the consequence of the political reaction to Fukushima will be a switch to other sources of energy, such as coal. Fukushima killed no one – even the fire fighters who dealt with it have no greater risk of dying from their work than ‘white van man’ in the UK – but the Chinese coal mines admit to killing 2,433 people in the last year. And that excludes long-term harm such as silicosis. If we try to decide what an ‘acceptable risk’ is narrowly and locally, we are likely to overreact and create greater risk elsewhere.

This then should guide the formation of engineers. All engineers should understand the need for trade-offs between the different requirements, including safety, of complex engineered systems and should be able to communicate those trade-offs across disciplinary and industry boundaries to those who authorise, regulate and fund their work.

5. View from the safety specialists: Allan Bain CEng, Development Director, Safety and Reliability Society

Communication across sectors is essential: SaRS exists to allow different industries and sectors to communicate. The issue of ownership of a risk is key when different industries are working together.

Safety emerges from a complex system – it is not a simple issue that can be dealt with by plugging in a simple procedure.

Engineering loses knowledge and skills as experienced engineers retire – corporate memory is essential for managing risk. The mobility of the engineering workforce is also a challenge to the safety culture in engineering, with engineers learning different approaches in different roles.

SaRS exists to provide focus, improve rigour and (in partnership with others) help to improve professional engineering standards – sharing lessons across sectors.

The aim of SaRS is not to set up new schemes for safety, but to create a framework that makes sense of existing schemes. It recognises that there are many routes to professionalism, and that there is no single scheme that can make a safety professional.

Competence in safety is gained by understanding the mechanisms of failure. There must be a cross-professional agreement on the body of knowledge needed, the appropriate standards and the standard methods for dealing with risk.

SaRS has been engaged in creating:

- A mechanism for retirees to pass on knowledge.
- A process to peer-review individual competence.
- Competence = training + knowledge + experience + ability + judgement + attitude.
- Facilitate EC-UK registration (for those needing it).
- Peer review what academia is teaching.
- A vision: passports (for generic safety and reliability professionals, critical thinking, safety culture) with industry visas.

The SaRS framework can allow standardisation of competency. It identifies five thematic areas of competency in:

1. **Underpinning** science, design, fundamentals of technology and basic safety for engineers or equivalent underpinning discipline knowledge.
2. **Availability and reliability** theory, analysis techniques, tests and trials, standards.
3. **Generic safety engineering** systems engineering, culture, risk assessment techniques, collating evidence, auditing, human error, proving mitigation.
4. **Management and interpersonal skills** knowledge management, leadership, quality, configuration, ethics, communication and influencing.
5. **Elements unique to the domain** standards, legislation, working practices, technology failure mechanisms; domain techniques.

An industry-wide standard is key and will be central to ensuring the profession works together across boundaries.

6. View from the profession: Jon Prichard, CEO, the Engineering Council

The lessons from the Nimrod review echo lessons from previous events for engineering safety – such as those of the Columbia Accident Investigation Board reports. There are clearly lessons that still must be learned.

In the management of enterprise risk, there are three components of risk to be managed: strategic risk, project risk and operational risk. These risks are to be managed at three levels: that of the individual, the team and the organisation. These have to be managed with the right systems, the right structure and the right culture, bringing together enterprise values, professional values and client values. Throughout, this is a process of creating a holistic approach to these different elements of risk and their management.

The professional engineering institutions can help to promote this approach by acting as qualifying bodies for safety professionals, ensuring engineers have the skills to manage risk and as learned societies promulgating knowledge and expertise in this area.

In the UK, the Engineering Council promotes the skills needed for management of safety by setting out in the UK Standard for Professional Engineering Competence the competencies and commitment to safety needed by engineers. It is seen as a leading global exemplar in setting

standards. Registration depends on experience; requires continuing personal development to keep experience up to date; and depends on showing a commitment to taking responsibility for managing risk and ensuring the health, safety and welfare of systems and those who work in them.

The engineering institutions provide a wealth of guidance on risk. The profession is self-regulating, and should be so, using and sharing its expertise to ensure that the best standards are met. The goal of the profession now is to ensure that the many elements of the engineering profession pull together to create a coherent approach to developing competence in engineering safety, and enacting a common set of values for engineers.

7. Forward plan

The outputs of this meeting are under active discussion within the engineering profession and a forward plan of action is being produced to promote debate and take forward the issues in question.