

THE FOUR PRINCIPLES OF PRODUCT SAFETY

*N.Sibley**, *B.Walby †*, *D.Priestley ††*

**BAE SYSTEMS, UK, nick.sibley@baesystems.com, †BAE SYSTEMS, UK, bill.walby@baesystems.com, †† BAE SYSTEMS, UK, duncan.priestley@baesystems.com*

Keywords: Product, Safety, Accountability, Conforming Products, Learning and Sharing.

Abstract

“Products” take many forms – tangible products like aircraft or bridges, intangible products like software or licences and services like maintenance or cleaning. If any of them are unsafe, the victims are frequently not the people who design, build or supply the product but the customers, users or third parties. Product safety management is therefore often quite different from the more mature and understood activity of workplace safety management.

This paper provides some of the findings from an industrially funded review of Product Safety practices across a number of sectors and identifies 4 Principles of Product Safety that span the sectors included in the review.

1 Introduction

In 2010 BAE Systems conducted a review of the management of Product Safety across all its sectors. The review examined many issues associated with the safety of the company’s Products and consulted widely with its businesses around the world.

The outcome of the review was a set of four principles of Product Safety:

1. Accountability
2. Level of safety
3. Conforming products
4. Learning and sharing information

The principles were tested by examining how six other sectors (automotive, civil aviation, construction, health, offshore, and rail) address their equivalent challenge. Similar principles were identified in each sector.

As with many significant systems engineering outcomes, the apparent simplicity of the four principles belies a significant effort by subject matter experts in Product Safety, Law and Systems Engineering.

This paper will explain the four principles and provide detail of the associated research and findings.

2 Approach

There were two significant stages in the approach used to better understand how the management of Product Safety could be improved.

- 1 Internal review of BAE business approaches, across all its sectors
- 2 External review and comparison of how other industries approach the management of Product Safety

Internal review of Product Safety

The internal BAE Systems review of its management of Product Safety was conducted through a comprehensive examination of existing processes and policy in relation to current working practice and incidents that had occurred. Face to face meetings with BAE staff were a key element of this review. The review was conducted from 3 perspectives:

Perspective 1 - evolution of professional practice

How has the sector progressed from being a “craft”, relying on the personal skills and judgement of qualified individuals, through to a design- or process-led activity in which standards are imposed across all practitioners? This perspective helps to elicit information regarding the structure by which authorisation is granted to the practitioner.

Perspective 2 – safety management

How does each sector:

- Decide on the appropriate level of safety required of a product and expresses it in a form that is agreed by all involved in the procurement and supply of that product?
- Ensure that the agreed level of safety is achieved by the product and is sustained throughout its life?
- Measure and promote the culture within the workers necessary to sustain the agreed level of safety?
- Investigate incidents and accidents involving the product?

In each case the word “Product” is interpreted widely to include service.

Perspective 3 – approval and assurance

More generally:

- How are companies, organisations and individuals approved?

- How are products and processes approved and how this is managed?
- How is quality assured for products, processes and skills through the life of a product?
- What standards ensure that a company is competent to deliver safe products? For example, is certification to ISO 9000 or 9001 generally considered adequate or are higher standards adopted by the industry either voluntarily or by regulation?

External Review of Product Safety

In order to attain a broader understanding of how wider industry manages Product Safety the internal review was extended to six other industry sector studies:

1. Automotive
2. Civil aviation
3. Construction
4. Health
5. Offshore
6. Rail.

Stakeholders from each of these sectors provided information in the form of a study report that addressed the questions associated with the three perspectives described above. The reports provided were not in any way a comprehensive review of the issues in the sector.

Information from the internal and external reviews was then compared to identify areas common to each industry, and where differences occurred.

3 Findings – The Broad Messages

The internal and external reviews revealed commonality in the following areas

- Independent verification
- ALARP (As Low As Reasonably Practicable)
- Affordability
- Applicability of ISO 9000 and other Standards
- Safety Assessment
- Documentation of Safety
- Culture
- Change as a source of Risk
- Wider contributions to Product Safety

Independent verification

Verification is employed in several sectors to assure product safety. It is a valuable tool because it does not undermine the line of accountability for safety. The accountable person is responsible for establishing that the level of safety is appropriate. The verifier challenges the responsible person to set out the claim for safety and to present the evidence that justifies that claim. Verification ensures that the evidence justifies the claim. One sector has a formal definition of this:

‘confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled’

To be effective, the verifier must be objective and impartial. This is usually expressed as a requirement for independence. This does not have to mean that the verifier is employed by a different company; the rail industry has a legal definition of independence that states in summary that an independent verifier is:

- Competent - has sufficient skills, knowledge, experience and resources
- Uninvolved - has not been responsible for the product being assessed
- Objective - is sufficiently independent of the management system for that product.

If they are in conflict, competence should take priority over independence.

Reducing risks to a level that is As Low As is Reasonably Practicable (ALARP)

The requirement to make risk levels ALARP is a requirement of the criminal law in many countries, including the UK and, at least for workplace safety, Australia, India and New Zealand. It is also the requirement of the civil law in those countries and the USA.

The ALARP philosophy pervades the sectors included in the review. The construction, offshore and rail industries adopt ALARP. The medical sector, at least for devices, is driven by a similar condition by the European Directive. The civil aviation community is increasingly looking to a similar test to decide if a risk is acceptable. It is only in the automotive sector that it does not appear, reflecting perhaps a societal view that automotive risks are consciously accepted by motorists and hence are driven down by the market rather than an external objective.

Affordability

A common theme through the sectors is that cost is one of the factors that are taken into account when determining the target level of safety. For example, car manufacturers set a level of safety determined by market expectations, health economics is primarily concerned with optimal allocation of finite resources and rail only implements safety measures that are reasonably practicable. Implicit in these is that the level of safety must be affordable.

The word “affordability” can cause some confusion in countries that allow a defence in criminal proceedings that a safety measure was not reasonably practicable. A company may not say that it could not afford a safety measure that other companies could have afforded – the financial circumstances of the defendant company are not relevant. This is not the same as the government of a country setting a budget for a product that limits the level of safety that can be achieved.

Applicability of ISO 9000 and other Standards

Many sectors require companies that supply products to be accredited to ISO 9001 as a minimum. However, this is not usually regarded as adequate on its own. The accreditation body is also important; for example the offshore sector requires accreditation by a body that it is itself accredited by UKAS. There is a parallel in medical devices, where the expertise and rigour of the Notified Body that assesses the device is important. The automotive and aviation sectors both set their own standards that follow the general form of 9001 but are more demanding.

The automotive sector also has its own standard for electronic control systems, because IEC 61508 is not considered suitable. The reasons include that its electronic systems are embedded in the product, not an external safety measure. Rail also defines special standards, in the case of the US being highly prescriptive.

Safety assessment

The ISO standard approach to risk management is widespread, following the classic sequence of: hazard identification, risk estimation, risk acceptance, management of mitigation measures, all in a closed loop to ensure that hazards remain properly controlled. The “risk acceptance” step relies on an accepted level of safety; risks are accepted if the target level of the safety of the product is achieved. In many cases this is a combination of a minimum level of safety that must always be achieved and a further requirement that all reasonably practicable risk-reduction measures have been implemented – the so-called ALARP requirement. Even in sectors where ALARP is not mandated, such as aviation, it is increasingly being adopted. It is informed by risk modelling, either quantitative as in the aviation and rail sectors or more qualitative as in health.

Documentation of safety

Most sectors require that the information relevant to product safety be properly documented. This is at the core of the construction sector’s regulations, and is a legal requirement for medical devices. Many sectors require a formal safety case and mandate a Safety Management System that includes skills of the people involved and processes that they follow.

Culture

Successful safety regimes have addressed the culture in which they operate. The offshore regime makes express reference to a just culture, in order to encourage openness - sharing experiences and report incidents. There are confidential reporting regimes (e.g. civil aviation, rail) that also encourage reporting of incidents such as near misses. The regime with the worst product safety record of those considered – health – has an anonymous reporting system that does not allow incidents to be investigated other than by the employer. The health sector also has a strong individualist culture, manifested by the unwillingness to proceduralise treatments with checklists.

An important aspect of culture that comes out in some of the sector studies is the need to engage the workforce. Product safety is one of the attributes of the Product, not a “bolt-on”, and emerges from the behaviours and attitudes of the people who conceive, design, build and support the product.

Change as a source of risk

Several of the sector studies identify change as a source of risk, for example in the “Compliance” section of the offshore study and when dealing with degraded modes of operation in rail.

Wider contributions to Product Safety

Product Safety is a consequence of many aspects of projects. There is a good example in the construction study where a procurement decision led to a major lapse of product safety in which several people were killed. The automotive sector recognises the importance of the marketing inputs to a car, as well as through life support and efficient recall. In health there is great benefit to be had from standardisation and general management. The offshore sector has found value in engaging the workforce in safety planning (this might also be seen as a cultural issue). In rail, the drive to open up markets has led to formalising safety management.

4 A Way Forward – The Principles of Product Safety

During the initial internal review of Product Safety management with in BAE Systems, 4 Principles of Product Safety were identified that underpinned good Product Safety management. These Principles were mapped to the detailed output from the external review and were found to be applicable across all the sectors that had been evaluated. The 4 Principles are:

Principle 1: Accountability

We shall work with our customers and others to ensure that there is, at all times through the life of every product, accountability for its unintended effects on the safety of people:

We are and remain accountable for those aspects of our products that are under our control or for which we are legally responsible

We shall make reasonable efforts to maintain accountability when we no longer have control of, or responsibility for, our products.

The Company’s accountability will be delegated to individuals.

Principle 2: Level of Safety

We shall work with each customer to agree the level of safety that is to be achieved by each product through its life.

We shall seek the highest level of safety of those who might be unintentionally harmed by the product that is compatible with the product's required performance, cost and schedule and the way that it will be used.

Principle 3: Conforming Products

We shall ensure that our products conform to their definition:

- With internal and, where necessary external, approvals for the organisation and product
- By deploying suitably qualified and experienced people
- By applying independent assurance.

Principle 4: Learning and Sharing Information

We shall work with our customers and suppliers through the life of each product to:

- Provide topical information on safety so that each customer may determine how the product is used
- Obtain information on the use and performance of the product to assess the consequences for safety
- Understand the cause of significant accidents and incidents involving our products, where appropriate with independent accident investigators, to reduce the probability of recurrence.

We shall seek to learn from other parts of the company, organisations and domains.

5 Conclusions and recommendation

Conclusions

1. All of the Product Safety Principles are adopted in all of the sectors considered. This shows that all of the set of Principles are necessary.
2. Nothing emerges from the sectors considered that is missing from the Principles and would be considered sufficiently fundamental to be another Principle. This shows that the set of Principles is sufficient.
3. There are useful lessons to learn from other sectors on how to implement the Principles. These are common themes which are not significant enough to be regarded as Principles but which should be considered systematically as drivers for effective Product safety; for example:
 - The need for a just culture
 - The use of independent verification and independent advisers
 - Adoption of the ALARP measure of acceptable risk.
4. In some case the parallels between the sectors are surprisingly strong. For example, the list of questions that the UK regulator asks when deciding if a medical device is acceptably safe translate almost directly into equivalent questions for defence, even to an equivalent of UORs

Recommendations

The review provided value in examining how other sectors deal with the equivalent of Product Safety, although only scratched the surface of a rich seam of evidence. Some of the people from those other sectors have shared that view

A programme of work could be developed to take this work further, with three themes:

- Greater global coverage – the sector studies do draw on evidence from other countries but are predominately UK based
- Greater depth – some issues have not been addressed at all, for example the observation that motor racing might provide a better model for BAE Systems than mass manufacture of automobiles because of the drive for performance
- Greater generalisation – this has been driven by a specific perspective of an aerospace and defence company; there might be great value in establishing a broader community of interest to share lessons and experiences.

The overall goal is to establish an exemplar for the management of Product Safety by which all companies may further improve their own practice.

Acknowledgements

This paper has been compiled based on a report produced by Dr Chris Elliott, Pitchill Consulting Ltd, who was the primary contributor to both the internal and external company reviews.