The Safety Case, its Development and Use in the United Kingdom

J. R. Inge, MEng CEng MIET; Ministry of Defence; Bristol, UK

Keywords: Safety Case, Assessment, Management

Abstract

In 1974 the United Kingdom adopted new legislation to govern the health and safety of people in the workplace and those that may be affected by workplace activities. The legislation recognises that good safety management is a matter of balancing the benefits from undertaking an activity and protecting those that might be affected directly or third parties.

The legislation requires that the risk of harm be reduced 'so far as is reasonably practicable' and that those managing the risks demonstrate their understanding and adequate management of that risk. It has given rise to a recognised means of assessing risk and demonstrating that there is satisfactory management in place, through the presentation and maintenance of a safety case.

This paper shows how different UK industries have developed and adapted the concept and principles of the Safety Case to demonstrate their understanding and management of risks within their business.

Introduction

In the UK up until the mid-1970s management of the safety and welfare of people in the workplace was controlled by a plethora of prescriptive rules and regulations. These had been adopted as industry knowledge and experience developed in response to events over the two hundred or so years since the Industrial Revolution. Following the introduction of steam driven plant in the eighteenth century a significant number of accidents and deaths over many years led designers to adopt standards to control the design and testing of boilers. Eventually many of the essential requirements for pressure vessels became formalised as legislation. Similarly as the use of electricity became more prevalent so the adoption of rules and standards led to the formation of laws for electrical installations.

Legislation developed in this way was reactive and even from the earliest days struggled to keep pace with innovation and the development of new technologies. In the 1960s the UK government took a new look at how safety in the workplace might better be addressed. A commission chaired by Lord Robens was tasked to examine the issue. The commission recognised that although it was possible for legislation to keep abreast of new developments (providing sufficient resource could be made available), a broader problem existed. The legislation of the time was complex and tackled safety piecemeal, with different rules for each type of technology or activity. A new, simpler way of managing safety was required, that ensured that the safety of the whole of an undertaking was addressed, not just isolated elements that fell under various specific statutes (ref. 1). As a result of Robens' report the UK decided to adopt a new legislative framework to govern health and safety. On July 31, 1974 royal assent was given to the Health and Safety at Work etc Act (ref. 2).

Health and Safety at Work etc Act 1974 (HSWA)

The HSWA adopted a holistic approach to the health, safety and welfare of workers. For the first time, legislation also explicitly addressed those outside the workplace that might be affected by work activities. The Act takes as its approach the concept that any situations that may give rise to harm need to be recognised and suitable measures put in place to eliminate or reduce the potential for harm. It set up two new organisations to oversee its implementation: the Health and Safety Commission (HSC) and the Health and Safety Executive (HSE). The HSE is the executive organisation that enforces the provisions of the HSWA, while the HSC protects health and safety at work in the UK by conducting or sponsoring research, promoting training and providing advice and information. The Commission also proposes new regulations and approved codes of practice under the authority of the Act.

The HSWA places a set of general duties on the person responsible for the activity (the Duty Holder), those undertaking the activity (usually the employees), and those supplying material and equipment for use in the workplace:

- Duty Holders provide safe equipment, working environments, systems of work, and arrangements that ensure safety and the absence of risks. To support this they must produce a health and safety policy and provide necessary information, instruction, training and supervision for their employees. They must also cooperate with the employees' safety representatives to develop these arrangements and check that they are effective. The act prevents employers from charging their employees for safety measures.
- Employees have a duty to take reasonable care for their own health and safety and that of others who may be affected by their acts or omissions. They must also cooperate with the Duty Holder in implementing safety measures. There is a general duty not to interfere with or misuse anything provided for health and safety reasons.
- Suppliers providing equipment for use at work must ensure that it is safe and without risk to health during its use and maintenance. They must test that this is the case, and provide adequate information to support safe use and maintenance.

The standard of risk reduction required in carrying out these duties is that the potential for an undertaking to cause harm is reduced 'so far as is reasonably practicable'. The HSE usually consider that this can be achieved either by following an approved code of practice (where a suitable code exists), or by conducting risk assessment to show that the hazards involved in an activity have been considered and adequately controlled. Further risk reduction must be carried out unless the cost of the reduction measure (including non-financial factors such as time, trouble or loss of capability), is grossly disproportionate to the safety benefit gained. This is often referred to as the ALARP principle – that risks should be reduced to a level that is As Low As Reasonably Practicable.

The HSWA sets the goal that activities should be safe and free from risk, but does not specify how this should be achieved. The Act itself is not worded to be specific to particular technologies or activities, but it may be extended through regulations when specific statutory measures are required. This gives the Act a flexibility that allows it to be applied to many different situations, in a way that is proportionate to the risk involved. In some cases, where simple systems are involved and the level of risk is low, the requirements of the HSWA can be carried out purely informally, for example written documentation of risk assessments is not required for organisations with less than five employees. More normally however, it will be necessary to show evidence that justifies why a system or activity is safe. This has led to the development of the safety case concept as a means of demonstrating why something is safe.

Safety Case Basics

Although different industries have developed different safety case regimes the basic principles are the same. A safety case can be defined as 'A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment' (ref. 3). The two elements – argument and evidence – are mutually supporting. The evidence is needed to justify that the argument holds true. The argument is needed to show that the evidence is sufficient and relevant, and that it actually supports the case for the safety of the system.

Typically, areas covered by a safety case would include:

- The scope of the system or activity being addressed, together with details of its context or environment.
- The management system used to ensure safety.
- The requirements, legislation, standards and policies applicable, with evidence that they have been met or complied with.
- Evidence that risks have been identified and appropriately controlled, and that the residual level of risk is acceptable.
- Independent assurance that the argument and evidence presented is sufficient for the application in question.

The detail of the safety case will be likely to show that the system is (or will be) designed to be safe, and that this safety is preserved through manufacture, operation, maintenance and eventual disposal. As well as the design itself, it is likely to consider the analysis and processes used in the design and the competence of the people involved. The

results of testing or prototyping, inspections or audits, and records of accidents or incidents observed during operation will also form part of the body of evidence.

A key part of the safety case will be to demonstrate that risks have been suitably managed. This will include justifying that all credible hazards have been identified and the corresponding risks have been assessed and reduced to a level that is both acceptable and ALARP. To do this, evidence must be presented to show that all the planned mitigations (such as design changes, training, documentation or procedures) are actually in place, and performing as intended.

A safety case might cover a small aspect of a system's operation, or its whole lifecycle. Safety cases can also be constructed to cover changes to existing systems or ways of working. For complex systems, the body of evidence making up the safety case can be vast. In a high-integrity system such as an aircraft, where each part was inspected before assembly, this might include the quality control records for every single rivet! For this reason, safety cases for reasonably complicated systems are not normally assembled as single physical documents. Instead, safety case reports are generated to summarise the argument for safety, and refer out to where the relevant evidence can be found. While the safety case constantly grows and evolves, the safety case report provides a snapshot of its status at a moment in time.

Safety Cases in UK Industry

The HSWA does not specifically require production of safety cases, but their use has become increasingly widespread across UK industry. In particular, they have been adopted in high risk industries where there is a requirement to demonstrate to regulators and the public that the activity is safe before it is allowed to take place. Such requirements have often been introduced through regulations, as a response to specific accidents. Prime examples are the UK nuclear, chemical, offshore, and railway industries. In these instances a satisfactory safety case must be presented to the industry's regulatory body before a licence to operate can be obtained. The same approach is now being adopted by other high risk industries such as civil aviation.

Nuclear: In the nuclear industry, the requirement for safety cases was realised in the late 1950s, following a significant release at the Windscale nuclear reactor in Cumbria in 1957. To try to prevent such an accident happening again, the industry started to set performance standards for safety, supported by formal risk analysis to show that the targets would be met. This was the forerunner of the safety-case approach. The Nuclear Installations Act 1965 introduced a licensing regime, one of the conditions of which includes production of safety cases justifying safety during all phases of operation (refs. 4 & 5).

Chemical: In 1974 an explosion at the Nypro chemical plant in Flixborough killed 28 people, injured hundreds, and damaged over 2000 buildings, shops and factories (ref. 6). The investigation into the accident led to the establishment of the Advisory Committee on Major Hazards by the newly-formed HSC. The committee drew its membership from government, industry and the trades unions, and drafted of a set of regulations for hazardous installations. Before these could be enacted, another major accident occurred: a large quantity of dioxin was released into the atmosphere in 1976 near the Italian town of Seveso, causing skin damage to over 400 people, killing over 3000 animals and leading to the slaughter of over 80,000 more (ref. 7). The resulting European Community directive was based on the British work, and enacted in the UK by the Control of Industrial Major Accident Hazards (CIMAH) Regulations 1984[1]. Key among its requirements was the production of a safety report demonstrating adequate consideration of dangerous substances, potential accidents and provision of effective safety management systems; effectively a safety case.

Offshore Oil and Gas: Safety cases were introduced for the offshore hydrocarbon industry following the recommendations of Lord Cullen's report into the Piper Alpha oil rig explosion and fire in 1988 (ref. 8). The Offshore Installations (Safety Case) Regulations 1992 (and 2005) require safety cases to be submitted to the HSE that demonstrate that major accident hazards have been identified and the risks to people reduced to the lowest level that is reasonably practicable. They also require demonstration that adequate audit arrangements have been established and other statutory requirements will be met. The regulations are goal setting in that they specify the

[1] Now superseded by the Control of Major Accident Hazards Regulations 1999.

scope and content of the safety case, but do not prescribe particular methods of meeting their requirements (refs. 9 and 10).

Railways: Prior to the 1990s, railway infrastructure, stations and rolling stock in the UK was operated as a nationalised industry by British Rail, with a central safety and standards setting organisation. Despite having a unified approach to safety across the organisation and over 150 years of industry experience in safety matters (ref. 11), several major accidents had raised public concern. 27 lives were lost in the 1987 fire at King's Cross underground station and the crash at Clapham in 1988 killed a further 35 (ref. 12). These events and the prospect of privatisation and the splitting up of the industry prompted a requirement for a safety case regime, and gave rise to the Railways (Safety Case) Regulations 1994[2].

These regulations recognised that the railway network would be operated by a mix of different commercial organisations with varying responsibilities. They imposed a modular system with railway safety cases supported by station and train safety cases. As with the Offshore Regulations, the Railways Regulations specify the required contents of the safety cases, without detailing the specific standards or techniques to be applied.

Safety Cases for Military Systems

Successive UK Secretaries of State for Defence have adopted the policy that where the Ministry of Defence (MOD) has been granted specific exemptions, disapplications or derogations from legislation, international treaties or protocols, it will introduce standards and management arrangements that are, so far as reasonably practicable, at least as good as those required by legislation (ref. 13). By the 1990s, the use of safety cases to manage civil systems had become established as good practice in high-risk industries. Although there was no legal requirement for safety cases to be produced for military systems the MOD started to adopt the concept of the safety case for establishing formal safety management for its systems during the mid-1990s. The Jones Report on Equipment Safety Assurance (ref. 14) recommended that a safety case regime be introduced to the procurement processes followed by the Ministry's Procurement Executive, and that safety cases should be introduced at the earliest possible stages of projects, as part of the project approval process. Safety cases were first applied to naval ships, followed a few years later by military land and air systems. They are now applied to all systems, both new and legacy.

The MOD has a single goal-setting Defence Standard for safety management across its activities, Def Stan 00-56, and uses a common core of processes such as hazard identification and risk assessment. However, because civil legislation and regulation varies between the land, sea and air domains, the actual implementation of safety management and the safety case regime varies across its operational domains, to give equivalence with the corresponding civil practice. These different regimes are described in a number of Joint Service Publications.

Ship Safety Cases: The UK's military ships fall into two main groups: the warships of the Royal Navy and the support vessels of the Royal Fleet Auxiliary. The Navy's combat forces are intrinsically military ships that are generally designed and built to meet military standards. The Auxiliaries include the logistic ships that support the fighting forces. These are governed under civil maritime regulations and increasingly often are built to commercial standards.

Safety Cases are required by JSP 430 to show sufficient evidence that safety requirements have been met and that risk has been reduced to a level that is ALARP and either broadly acceptable or tolerable. The safety case must also demonstrate that certain key hazards areas have been addressed, such as stability, structural strength, escape & evacuation, propulsion & manoeuvring, fire safety, explosives and further areas for submarines. These key hazard areas are regulated by Naval Authorities through a certification system. Demonstration of safety in the various areas can be either risk based or through compliance with prescriptive standards. In some cases where there are no special military issues, the requirement for a key hazard certificate may be met through equivalent civilian mechanisms, such as obtaining statutory certificates or being in class with a recognised classification society. In other cases, such as for explosives, there may be no equivalent civilian mechanism, or there may be a need for additional supplementary evidence (ref. 15).

---

[2] The UK railway safety case regime is being superseded by a system of certification and authorisations under the Railways and Other Guided Transport Systems (ROGS) Regulations 2006, to harmonise British and European rail safety legislation. Current safety cases will be phased out by October 2008.

Land Systems Safety Cases: Safety cases for land systems (e.g. a communications device, weapons system or armoured vehicle) comprise three parts. The first part is based on a high level assessment of the concept and early feasibility studies. It is used to set the safety requirements (Regulatory, Technical and Goals) the system must meet and to identify any areas of particular safety risk that might threaten the project. The second part of the safety case demonstrates that the design meets its safety requirements, qualifies the residual risk and identifies the controls and mitigations needed to manage those risks. This part of the case should be agreed by the time a system goes into manufacture or installation. The final element of the case assesses and demonstrates that all the mitigations and controls for managing and reducing residual risks are in place and effective when the system enters service. This would include maintenance and training regimes and management infrastructure such as reviews, incident reporting and configuration control. This three-part approach may form a future model for safety cases in other domains.

Air System Safety Cases: The MOD regulates military flying of its aircraft and the systems used to control them. Before aircraft are allowed to operate, a Release to Service Recommendation must be accepted by the MOD's Release to Service Authority. The recommendation is based on certification that the aircraft meets its airworthiness design requirements, supported by a safety case for the aircraft class and particulars for the individual airframe. In principle the safety case will cover all aspects of safety related to the aircraft's operation, however in practice they typically concentrate on airworthiness. It will also provide a description of the aircraft's safe operating envelope, identifying the limitations and procedures necessary to achieve the required level of safety.

As with naval and land systems, the methodology used for generating the safety case is that given in Def Stan 00-56, but specific requirements are given in JSP 533. The JSP details the key areas that the safety case should address at each stage of the MOD's CADMID project lifecycle (Concept, Assessment, Demonstration, Manufacture, In-service and Disposal). It requires that the safety case defines the aircraft's configuration and operating environment, its safety requirements, targets and attributes and its design. The safety case must also justify the design's airworthiness and detail the supporting evidence (ref. 16).

Pros and Cons of the Safety Case Approach

The safety case approach can be used very effectively to justify why something is safe, by providing a reasoned argument that is tailored for the situation in question. It gives the flexibility to allow the rigor of the argument to be proportional to the risks involved. When the body of evidence that makes up the safety case is used to underpin a structured argument, it becomes easy to see how the argument is affected if evidence changes, or new evidence becomes available. The approach can also respond to new innovations and changes in best practice.

A main disadvantage of the approach is that it can be very difficult to determine precisely what level of evidence is sufficient for a given system. This becomes an engineering judgement, based on the experience of those managing safety and their advisors. The safety case approach requires a greater degree of competence from those involved in it than does a prescriptive approach to safety, where managers can achieve compliance by following rules rather than making decisions.

References

1. Lord Robens. Safety and Health at Work. Report of the Committee 1970 - 72. Cmnd 5034. London: HMSO, 1972.
2. Health and Safety at Work etc Act 1974. Elizabeth II 1974. Chapter 37. London: HSMO, 1974.
3. Ministry of Defence. Defence Standard 00-56 Safety Management Requirements for Defence Systems. Issue 4. Glasgow: UK Defence Standardization, 1 June 2007.
4. Health and Safety Executive. The Licensing of Nuclear Installations. March 2007. HSE: http://www.hse.gov.uk/nuclear/notesforapplicants.pdf
5. Health and Safety Executive. Nuclear Site License Conditions. HSE: http://www.hse.gov.uk/nuclear/silicon.pdf
6. Department of Employment. The Flixborough Disaster: Report of the Court of Enquiry. London: HMSO 1975.
7. Wikipedia. Seveso Disaster. http://en.wikipedia.org/wiki/Seveso_disaster
8. Lord Cullen. The Public Enquiry into the Piper Alpha Disaster. 387–390, London: HMSO November 1990.
9. Offshore Installations (Safety Case) Regulations 1992. S.I. 1992/2885

10. Offshore Installations (Safety Case) Regulations 2005. S.I. 2005/3117.
11. Wikipedia. HM Railway Inspectorate. http://en.wikipedia.org/wiki/HM_Railway_Inspectorate
12. On this Day 12 December. 1988: "35 dead in Clapham rail collision." BBC: http://news.bbc.co.uk/onthisday/hi/dates/stories/december/12/newsid_2547000/2547561.stm
13. Browne, Des. Safety Health and Environmental Protection in the Ministry of Defence – A Policy Statement by the Secretary of State for Defence. 19 December 2006. http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/PolicyStrategyandPlanning/SosPolicyStatementOnHealthSafetyAndEnvironmentalProtectionsignedCopy.htm
14. Jones, R. E., and Lt Col H C Abela. Man S (Org) Study No 773 - Equipment Safety Asurance. London: Ministry of Defence, March 1994.
15. Ministry of Defence. JSP 430 Ship Safety Management. Part 1, Issue 3, Amendment 2. Bristol: Ministry of Defence, September 2006.
16. Ministry of Defence. JSP 553 Military Airworthiness Regulations. 1st Edition, change 4. London: Ministry of Defence, November 2006.