national research centre for
OHS regulation

RegNet
REGULATORY INSTITUTIONS NETWORK

Seminar Paper 2

Safety Cases: Success or Failure?

May 2002

Peter Wilkinson
Manager Review Implementation Team, Offshore Safety Section,
Department of Industry, Tourism and Resources

THE AUSTRALIAN NATIONAL UNIVERSITY

SAFETY CASES: SUCCESS OR FAILURE?

Peter Wilkinson

Synopsis

This paper sets out the historical background to the development of safety cases as a tool to manage and regulate major hazard industries, primarily in the UK. The main features of successful safety case systems are described and an assessment made of the successes and failures in their application.

The views expressed are those of the author and do not represent the views and policies of DITR.

Introduction

1. It is probably only possible to achieve absolute safety if as a society we do not undertake hazardous activities. However we know that the application of technology brings great benefits to us as a society. The skill comes in exploiting potentially hazardous technology whilst minimising the risks - accepting it is probably not possible to totally eliminate the risks.

2. The concept of using the mechanism of a safety case as a tool to help manage major risks, although around for some considerable time, particularly in the nuclear field, continues to expand into new areas. This alone tells us something about the worth and success of the safety case concept. This paper will briefly trace some of the history of its development in the UK and Europe, outline some of the features of successful safety case regulatory regimes as well as some of the difficulties.

3. In the context of this paper the term "safety case" is used to cover the variety of legislative requirements which variously require "safety cases" or "safety reports". The term "installation" is used to describe the site that presents the major hazard whether it be a nuclear power station, an oil refinery or an offshore oil and gas facility and the term "operator" to describe the owner or employer in charge of the installation.

History of Safety Cases in UK

4. What is the background to the growth of safety case type approaches to health and safety regulation? Almost 30 years ago Lord Robens chaired an inquiry into health and safety at work which led to the Health and Safety at Work etc Act and the formation of the Health and Safety Commission (HSC) and its operating arm, the Health and Safety Executive, (HSE).

5. The general approach of HSC/E is based on two important principles. Firstly those who create risks, particularly employers, are responsible for controlling them. Linked to this is the idea that regulations should set goals, rather than prescribing solutions. The second principle is that of reasonable practicability. In general we require safety standards to be "reasonably practicable". In other words controls should be commensurate with the risk. The word "reasonable" means that cost must be taken into account. The greater the risk, then the greater the amount of expenditure it is reasonable to expect employers to invest in to ensure that they have adequate controls in place.

6. Whilst we are talking about some principles of regulation, at this point I would like to say something about the following terms, prescription goal setting, and self regulation.

Unfortunately these terms are frequently used as if they are so well understood that no explanation or definition is needed. However the evidence is that although the terms are part of the everyday vocabulary of people interested in occupational health and safety they mean different things to different people. I am therefore going to add to the debate by offering my perspective.

Prescription

7. Prescription is usually taken to mean the introduction of detailed and mandatory regulations. Prescriptive regulations prescribe specific solutions. So for example in regulations on power presses, at one time you could find the following:

> no power press shall be used after the setting …..of the tools thereon unless a person appointed….has inspected and tested every safety device thereon …(Power Press Regulations 1965 UK)

8. These regulations, combined with effective enforcement by HM Inspectors of Factories, were widely credited with dramatically reducing the number of power press accidents. I doubt whether any detailed research was done to try and isolate the key success factors in reducing accidents, but my belief is that prescriptive regulation without an active regulatory body would not have had the same degree of success.

Goal Setting

9. Goal setting is not new and has been around since the earliest days of safety regulation in the UK. This type of regulation specifies principles rather than the specifics Although the Factories Inspectorate was established in 1833, it was really around the turn of the century that more effective legislation was introduced, this example, although from the 1960s was only a restatement of legislation from the early 1900s :

> Every dangerous part of machinery shall be securely fenced…
>
> (Factories Act 1961)

As can be seen it does not specify which parts have to be guarded (securely fenced), nor how.

Self Regulation

10. This is usually taken to mean the process by which an organisation regulates itself without direct intervention from a regulator. It is sometimes used as if it were a synonym for the safety case type of regulatory approach or even for "goal setting." However, as will become apparent later, the regulatory approach I mean in relation to safety cases is not self regulation, although it has some self regulatory features but nor is it prescription, although it also has some prescriptive features. I shall argue that effective safety case systems require elements of goal setting, prescription, self regulation **and** an effective regulatory body to make this work. I will come back to these points later in the paper.

11. An interesting feature of the Robens review and the developments it spawned was that they took place as a result of a planned review of health and safety regulation and not as a response to a disaster or newly identified health hazard. However in 1974, shortly after HSC/E was formed, there was a disastrous explosion at Flixborough. Several tonnes of cyclohexane escaped from the plant following a poorly executed process modification. 28 people were killed and 36 injured on the site. Another 53 casualties were recorded off it.

12. Following this disaster HSE set up a panel of experts - the Advisory Committee on Major Hazards - to study the control of major hazards and to advise on the best policy to adopt. They produced three reports, the first of which in 1976 proposed a three part strategy for managing major hazards. This consisted of:

    - identification,
    - prevention and control,
    - mitigation.

13. The **identification** of installations presenting, or liable to present, a major hazard involved two factors : the recognition of this fact by the operator concerned and the notification of it to the relevant authorities. Measures of **prevention and control** involve operators assessing their processes in order to determine the hazards and risks; and then using this information to ensure that appropriate precautions are taken to secure safe operations. **Mitigation** measures include separating vulnerable populations from hazardous installations through land use planning controls; on- and off-site emergency plans to provide for effective response to major accidents; and warning the general public about the potential hazards and the action to take in an emergency.

The Seveso Directive

14. This strategy was to have been backed up by regulations. However the major environmental disaster at Seveso, Italy in 1976 led to a European directive - the so called "Seveso" Directive which was significantly influenced by the emerging UK ideas. The Directive led in UK to the Control of Industrial Major Accident Hazards Regulations (CIMAH) in 1984. CIMAH required manufacturers to prepare a written safety report containing details of the dangerous substances, the installation, the management system, the potential for major accidents and the measures to be taken to prevent, control and minimise the effects of major accidents. At the time it was a new and radical approach, making manufacturers look at their sites and requiring them to make their own assessment of risk potential and control. However a direct line can be traced back to the principles established by the Robens inquiry which reported in 1972 and which are summarised above. CIMAH was amended in 1987 following the Bhopal disaster in India and again in 1988 following the 1986 Sandoz Warehouse fire in Switzerland. The Control of Major Accident Hazard Regulations (COMAH) is the natural successor to CIMAH, and COMAH safety reports are now being produced.

Nuclear and Offshore Industry Safety Cases

15. In the nuclear field safety cases have an even longer history. The Nuclear Installations Act 1965 requires all nuclear plants to obtain a licence from HSE prior to operation. One of the standard licence conditions requires the production and maintenance of an adequate safety case. As with the non-nuclear industrial hazard regimes, a primary aim of the safety case is to reduce the probability of a major incident occurring. Although different in detail from the other safety case regimes, the fundamentals are the same. Similarly for Britain's offshore oil and gas industry which came relatively late to safety cases, following the Piper Alpha disaster in 1988, in which 167 men lost their lives. Unfortunately the offshore industry had been insulated from the development of safety cases as a tool for managing major accident hazards. Lord Cullen's inquiry into the Piper Alpha disaster carefully considered and endorsed the safety case concept which was subsequently applied to the industry by HSE's Offshore Safety Division. Australia considered the applicability of the Cullen Report to its offshore hydrocarbon industry and also decided to implement a safety case regime.

Principal Feature of Safety Case Systems

16. The main requirement of all safety cases regimes is that via their safety case, operators must demonstrate that they have identified and assessed all the relevant risks and have taken all the steps necessary to reduce these risks to a level as low as is reasonably practicable (ALARP). The key common features of all UK safety case regimes are:

- Safety cases must be produced by the operator of an installation,
- The safety case must identify the safety critical aspects of the installation, both technical and managerial,
- Appropriate performance standards must be defined for the operation of the safety critical aspects,
- The workforce must be involved,
- The safety case is produced in the knowledge that it will be scrutinised by a competent and independent regulator who may prohibit the activity if there are serious shortcomings in the case.

Safety case prepared by the operator of the installation

17. The principle here is that those who create the risk must manage it and it is the operators job to assess their processes, to identify and evaluate the risks and implement the appropriate controls. They have to carry out the analysis of the risks presented by their plant and not the regulator. Whilst there may be a wish in some quarters for regulators to duplicate the activity of the operator, in practice the regulator can never be there all the time and even if they were they do not have the responsibility to operate it. Only the operator can have the in depth knowledge required to manage the installation safety. So the operator manages the installation, analyses what could go wrong, puts in appropriate controls both hardware and managerial controls - all of which are then intelligently challenged by the regulator.

Safety Cases must identify the safety critical aspects of the installation

18. Successful safety cases must identify the safety critical aspects of the installation, including the technical and managerial issues. A safety case which focuses on one of these aspects at the expense of the other will be flawed. Analysis of disasters almost always shows a combination of technical and managerial flaws which have led up to the event occurring.

Performance Standards for the safety critical aspects

19. A "performance standard" is a statement, which can be expressed in qualitative or quantitative terms, of the performance required of a system, item of equipment, person or procedure, and which is used as the basis for managing the hazard through the life cycle of the installation. Performance standards underpin a safety case system. Without performance standards operators and regulators can neither assess nor measure the performance of the duty holders systems - technical or managerial.

20. An important principle in setting performance standards is that their number and level of detail should be commensurate with the magnitude of the risk being managed. From the perspective of risk management there is little to be gained from setting performance standards for systems or sub-systems or components of systems that contribute little to the management of overall risk reduction.

Workforce Involvement

21. To prepare an adequate safety case requires a range of skills and knowledge. However it is unlikely to be successful in achieving its aims if it does not take advantage of the substantial

knowledge of the work force. Their involvement is necessary because they are directly affected by an inadequate safety performance and will know what happens in practice and why. Furthermore developing a safety case, which includes a description of what, is done and why, can allow individuals to see how their individual effort fits into the bigger picture of operating the installation safely. This is of itself beneficial - making it more likely staff will do the right thing because they know why it is right rather then relying on a culture of staff doing what they are supposed to, because that is what the rules say. Involving the workforce in this way also frequently leads to the discovery of more efficient and safer ways of doing things.

A competent and independent regulator

22. Finally a successful safety case system must have a competent and independent regulator with adequate legal powers. The regulator must be competent so that the operator will carry out the process of preparing the safety case in a rigorous manner, in the knowledge that if it is not done properly it will be challenged by the regulator. This competence is also essential if the installation operator and - perhaps more importantly - those who may be affected by the installation are to have confidence in the judgements made by the regulator. Adequate legal powers must be available to the regulator to compel the operator to take appropriate remedial action where the case for safety has not been made. This does not mean that these powers will always be used or that use will be frequent. However it must be apparent to the operator that the powers are available and will be used if necessary. In this way it makes it more likely that the operator will take effective action in the first place - without the regulator having to intervene. And that when the regulator does intervene, improvements are achieved by persuasion rather than by compulsion.

Prescription, Self-Regulation and Enforcement

23. When I defined "self – regulation" at the start of the paper I said that the effective application of the safety case approach requires there to be elements of prescription, self – regulation as well as an effective regulatory organisation. To some this may seem paradoxical. In this case the "prescription" is not the traditional government imposed prescription but comes about as a result of the operator describing (or prescribing?) in their safety case how safety is to be achieved.

24. The operator is required to identify the hazards, assess the risks, introduce appropriate control measures and a system for managing them. Amongst other things these include procedures for isolation of plant, leak testing, making up joints in process pipework, permit to work systems and so on. It is for the operator to elucidate these control measures. Once accepted by the regulator this description of how the operation is managed becomes the law and it is an offence to operate the facility, otherwise than in accordance with the accepted safety case. The regulators role is to judge if the analysis of the hazards and risks are reasonable and if the control measures have the capability to work and then to see if they are applied and work in practice on the facility.

25. By my definition this process has elements of self – regulation and prescription but if it is to work effectively an adequately resourced regulator to ensure it is applied in practice is also required.

Benefits of Safety Cases

26. The benefits of safety cases come in a number of areas. These include:

- an improved understanding of the hazards and risks,

- an enhanced knowledge of the technical and managerial controls required to manage them, and,

- better oversight by the regulator.

Taken together these should lead to the principal goal of a reduction in the number and consequences of major accidents

Improved Understanding

27. Experience suggests that the main benefit of a safety case comes from the **process** that the operator has to go through to prepare the case. Thus it is not the document or suite of documents, called the safety case, that should be seen as the greatest product of safety case regulations, rather it is the process of preparing the case and the improvements in the hardware and managerial arrangements that are identified as necessary. The operator of the installation will always know it better than any regulator and the requirement to produce a safety case is intended to ensure that they know it even better.

28. Sometimes the preparation of the safety case is the first time that an operator has systematically analysed how the installation is designed, built and operated. Often the process of preparing the safety case has led to improvements being identified and implemented. In this sense there is an element of self-regulation which is directly in keeping with the conclusions of the Robens Committee on health and safety mentioned above.

29. These improvements have taken many forms, both technical and managerial although it is usually easier to identify the specific technical improvements compared with the less tangible improvements to managerial systems or the safety culture, although there is evidence for all these. For example, one operator, once they saw the safety case regulations on the regulatory horizon, decided they needed to rethink the type and location of their accommodation module. They decided to build an additional jacket (the name usually given to the support structure of a platform) and install a new accommodation module on it. This was then linked to the rest of the complex by a 70m bridge, the length determined by the predicted consequences of a riser failure on the main complex.

30. An offshore oil platform built in the 1970s had been modified to receive an additional pipeline from another field. Whilst preparing the safety case it was realised that there were excessive lengths of pressure relief pipe work without emergency shutdown valves. Any failure of the pressure relief pipe work would have had major consequences. The operator made appropriate modifications at a cost some £6 million. Similarly there is emerging evidence that as a result of preparing COMAH safety reports some operators have found they can reduce their inventories of hazardous substances. And this is before HSE has examined the case and discussed their findings with the operator.

31. One of the effects of the UK's offshore safety case system, reported by an independent survey of the industry was the improvement of safety management systems (SMS) and in some cases the SMS was formalised for the first time.

An Improvement Plan

32. There are few facility operators who would claim that their installation is perfect in all regards. Therefore there will always be areas, which can be improved. Preparing and reviewing safety cases provides both the driving force and framework by which areas of improvement can be identified and assessed, and programmes of action prepared and agreed with the regulator. In practice there can be few if any safety cases, which can be regarded as, complete. This is of course entirely consistent with modern thinking on quality in general,

which often emphasises the importance of "continuous improvement". Examples of these include the programmes of work agreed by HSE with the operators of nuclear power stations with Advanced Gas-Cooled Reactors, as a result of a regular review of the safety cases.

Improved intervention by regulators

33. Safety cases make it possible for the regulators interventions to be more efficient and effective. This is because the safety case should identify the safety critical issues and the regulator can concentrate on these. Furthermore the need to provide a good quality assessment of a safety case has led to improvements in the intervention processes in HSE.

34. Regulators use a variety of different intervention techniques which vary according to the circumstances. Briefly these include carrying out an assessment of the document or documents that constitute the safety case, verifying what happens in practice is consistent with the safety case, and investigating incidents which occur.

35. Typically the process involves a group of specialists who have particular skills and knowledge of the technology involved, including its management and knowledge of the particular installation. Depending on the circumstances there may be some verification of what actually happens on the installation compared with the safety case, before the case is accepted.

36. The amount of verification varies. In some cases, especially with new installations or with substantial changes to an existing installation, a great deal of verification takes place before the case is accepted. In other cases much of the verification is done in the "post acceptance" inspection or audit programme. The differences are ones of degree not principle. In all cases verification takes place, as we know from experience it is not unusual to find that the reality on the installation does not always match what was intended in the safety case. This can work both ways with examples of well managed installations submitting poor safety cases which do not do justice to the reality and poor installations with safety cases suggesting that conditions are rather better than they actually are.

Improvements to the regulators internal processes

37. The advent of new safety case type regulations such as COMAH and the UK's Offshore Safety Case regulations which preceded them, has helped to facilitate change within the Health and Safety Executive. Management structures have been reorganised and new processes developed to ensure a large number of safety cases can be assessed effectively and consistently within defined time limits. The same was true when safety cases were applied to the UK rail industry.

38. New systems founded on quality principles have been developed to control the assessment process. The required focus on delivering a carefully considered assessment within a defined deadline, has led to a renewed focus on project management skills, (an individual safety case is usually treated as a small project in its own right), and on arrangements to facilitate team working. To ensure the decisions on the acceptability or otherwise of safety cases are of high quality, new arrangements to peer review decision taking and to independently audit the processes have been introduced. Although a by-product of safety cases they are still a tangible benefit to HSE of applying a safety case system.

Lessons Learnt

39. HSE and the industries it regulates have experienced a number of difficulties in applying safety cases, these include the size and complexity of some cases with an associated lack of usefulness to an operators own work force, "stretching" probabilistic risk assessment

methods such as quantitative risk assessment (QRA) beyond its reasonable usefulness, and difficulties in explaining to the public and media, HSE's role where safety cases are accepted.

Size of and Detail in Safety Cases

40. One of the problems HSE has faced with the use of safety cases has been getting the level of detail right. Initially there was a tendency for HSE to press for great detail. This was because HSE inspectors wanted to ensure there was sufficient detail in the case for them to be able to judge whether the case for safety has been made and to enable enforcement action to be taken, if the operator does not do what is said in the case. The more general the statement, the more difficult it can be to make this judgement and to use it for enforcement. However the more detail the case contains, the larger the documents become and they run the risk of being less useful to the operators own staff. In the case of some of the older nuclear installations safety cases, there could be thousands of individual documents.

41. Early offshore safety cases suffered similarly. Part of the problem stemmed from the need to produce a document, which was striving to meet the needs of more than one "customer". In practice a balance has to be struck between the needs of the regulator and the operators own staff. Initially they have tended to be heavily orientated towards the need of ensuring acceptance by the regulator but latterly the needs of other audiences, including an operator's own staff, have received greater consideration. This has been achieved by developing "electronic" safety cases or by preparing high quality summary documents to help users "navigate" their way around the documents.

Quantitative Risk Assessment

42. Probabilistic techniques such as QRA have been widely used. Unfortunately, although it can be a very useful and informative technique, its use has sometimes been "stretched" beyond what the available failure rate data, will support. For example whilst there may be substantial data available on the failure rates on valves, it is not clear to what extent the data is equally valid for the very large and individually made shut down valves encountered at gas terminals and on offshore platforms.

43. In addition there have been some concerns that QRA has been used to justify situations that experienced engineers would deem unacceptable. In one case, on an offshore gas platform, the main export pipeline runs through a corridor adjacent to the accommodation block. QRA was used to demonstrate that the risks did not warrant any modifications. However good engineering practice suggested there were a whole series of measures, which should be taken to reduce the risks. Although it was deemed not to be reasonably practicable to move the riser or build another accommodation platform, the following changes were made:-

- blast walls were strengthened,
- automatic blow down system was fitted to reduce the potential for escalation,
- pipeline supports were strengthened to prevent fracture by explosion induced vibration.

44. QRA is a valuable tool, but because of the uncertainties it cannot be used in isolation, nor replace the use of good engineering judgement. Both approaches are important - the trick lies in getting the balance right.

Confidence in the Regulator

45. The public use several indicators to judge regulators. With public safety risks two indicators dominate: the number and severity of accidents and the amount of visible formal enforcement. On the former indicator the record speaks for itself but on the issue of

enforcement, safety case regimes can create a false impression of a low level of enforcement. This is because the public and the media only see the final product of the process - usually an accepted safety case. What they do not see is the extensive series of interactions between the regulator and the operator during which critical aspects of the safety case are vigorously challenged and as a result improvements made to the risk control arrangements. This challenge based dialogue is a robust enforcement process but steps need to be taken to explain this to the public and to make the process more transparent.

46. Another possible difficulty for regulators is that they may be seen by the public and media as being part of the problem when things go wrong - as they inevitably will from time to time. It is unrealistic to think that safety cases can guarantee to protect operators and society from major disasters - perfection is rarely possible. However if the regulator has accepted or in some way approved the safety case then they may be seen also to have failed in the event of a major accident. This of course would be right if the accident happened because one of the scrutinised and "accepted" control systems patently did not have the capability to achieve its stated goal. However experience suggests that this is unlikely. Usually accidents happen because operators fail to meet the standards they set themselves in their safety cases.

Measuring Success and Failure in Safety Case Systems

47. The ultimate test of success and failure of safety case systems is whether or not they reduce the frequency of major incidents. Fortunately they are relatively rare events anyway so it may be some time before we can definitively judge success or failure. Indeed HSE is only just starting to receive the safety reports produced as a result of COMAH. It will be the historians of health and safety who will have the privilege of making that judgement. However we do not have that luxury of time and we must make judgements as we go along.

48. The near universal opinion of managers and most of the work force at hazardous installations is that safety cases have been very successful. There are of course problems and I have discussed some of them above. However the problems are not ones which demonstrate any fundamental flaws in the concept, rather they are problems of applying the concept in practice and are thus susceptible to "fine tuning" of the system. This positive view of safety cases is endorsed by HSE's experience of applying safety case systems in the nuclear, onshore major hazards, offshore oil and gas industries and the railway industry. (The recent public inquiry into the Paddington train disaster endorsed the safety case concept.)

49. Positive though these views are, they are not enough to base a conclusion on. We need more and preferably independent evidence. HSE are obliged to assess the impact of all new legislation in terms of the costs and benefits to industry and the nation as a whole. In the case of the Offshore Safety Case regulations which followed the Piper Alpha disaster, Aberdeen University carried out a study to assess the costs and benefits. This was published in 1995. The study reports on the problems as well as the benefits of applying safety cases offshore. This paper has discussed some of these problems also. However the study concluded that the Safety Case Regulations have had;

> a positive impact on safety in the offshore oil and gas industry, particularly … a heightened awareness of and more focused attention on risk, improvements in the management of safety and the better targeting of safety related expenditure.

50. A follow-up study published in June 1999 gives more detail on the successes and failures, from a later perspective and hence more experience of the safety case system. However the overall positive conclusion of the success of the safety case system remains.

Conclusion

51. Safety Cases have been in use in the UK now for some time, as a technique to help manage the risks in the major hazard industries. There is enough experience to be able to form an overall judgement on their usefulness. They are not a panacea and they will not prevent all major accidents, nor less serious ones but they do seem to help us reduce the probability of a major event occurring and to mitigate the consequences of those that do occur. There are also problems in deciding the level of detail needed in a safety case. However all the evidence from across a wide range of industries and from the most senior to junior staff, as well as from independent evaluations points to their success and they have become the standard tool to manage major hazard industries.