

## **THE USE OF A SAFETY CASE APPROACH TO SUPPORT DECISION MAKING IN DESIGN**

W.A.T. Alder and J. Perkins  
Binnie Black and Veatch, Redhill, UK

In many of the high hazard industries the safety case and safety report approach is required under major hazards legislation. The benefit of the approach is the demonstration that the risks of an operation or a facility are reduced to as low as reasonably practicable and that continued operation is justified on health and safety grounds. The principles behind the development of a safety case are the development of an argument, the presentation of information to support the argument and a permanent record of that information for future use. These features are in themselves useful to organisations to assist risk management and possibly to meet wider requirements of the Health and Safety at Work etc. Act. The Safety Case approach has been adopted during in major infrastructure projects specifically to assist decision-making. The approach has been used to assess levels of safety management and residual risks with certain design options. In areas where there has been concern over health and safety aspects of the options, the safety case has been used as the forum for analysing and presenting the arguments for or against the options. A process of consultation with the stakeholders using the safety case has been carried out to gain agreement on which option to select.

Safety Case, infrastructure projects, CDM regulations.

### **INTRODUCTION**

Safety cases or safety reports are used widely in the high hazard industries for a variety of purposes, but principally to demonstrate the adequacy of safety of facilities or operations. Their production is required under a variety of Health and Safety regulations and other legal requirements.

The need for such a demonstration of adequacy is obviously due to the potentially disastrous consequences in the event of a major accident, and hence the need to be stringent in analysis of the potential for the accident to occur and the control of its likelihood and mitigation of severity.

However the concept of demonstration of the adequacy of safety has potential for application beyond the high hazard industries. In particular where approval or acceptance from a range of stakeholders is required, demonstration in the form of a safety case presents a useful way forward.

The authors have developed and used a safety case approach as a means of demonstrating the adequacy of safety of options during the design phase of projects, and as a vehicle for stakeholder consultation and acceptance. The particular applications in which it has been used has been in major infrastructure projects in the United Kingdom which are not subject to any of the UK major hazard legislation but are subject to the CDM (Construction Design and Management Regulations, 1990) and other safety regulations.

This paper discusses the broad issues of safety cases and the approach used by the authors and discusses the benefits and some of the problems of the approach.

## AN OVERVIEW OF SAFETY CASES AND SAFETY REPORTS

The high hazard industries are the principal users of safety cases or safety reports in the UK where legislation requires their production. The Control of Major Accident Hazards Regulations, 1999<sup>1</sup> (COMAH Regulations) require companies to produce safety reports if they operate or are intending to operate plant or processes that have inventories of hazardous materials exceeding certain threshold values. The Offshore Installations (Safety Case) Regulations, 1992<sup>2</sup> require a safety case for fixed and mobile installations for oil and gas extractions in UK waters, while the Railway Safety Case Regulations<sup>3</sup> require safety cases from a range of operators on the UK Rail networks. In the nuclear industry, safety cases are required to be produced under Condition 14 of an operators Nuclear Site Licence issued under the Nuclear Installations Act, 1965<sup>4</sup>.

The major requirement for all of these safety cases and reports is to provide a *demonstration* of the adequacy of safety with control measures in place to conform to the ALARP principle<sup>8</sup>. Safety cases have been defined as a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment<sup>9</sup>.

For example the COMAH regulations call for the safety case to demonstrate that major accidents are identified and necessary measures are taken. Demonstration in this case is intended to be “make the case/argument” rather than “prove beyond doubt”<sup>10</sup>. Views on the composition of a Safety Case under the earlier CIMAH regulations were that it should consist of facts about the site, reasoned arguments about the risk from the site and conclusions<sup>5</sup>. The offshore installations safety case regulations require that a demonstration that measures will reduce risks to as low as reasonably practicable. Nuclear site licence conditions phrase the requirement slightly differently in that a safety case consists of “documentation to justify safety” which amounts to a demonstration.

The role and purpose of the safety case in the Railway industry was considered in detail in the Ladbroke Grove Rail Inquiry. Many of the conclusions are applicable to safety cases used in any of the high hazard industries. In particular Lord Cullen, in his report following the inquiry<sup>6</sup>, notes that a safety case is seen as providing an appropriate means of managing safety and providing an adequate assurance of safety by independent reviewers. He also notes that a safety case should show how the duty holder has reduced the risks associated with its operation to as low as reasonably practicable. During the inquiry evidence, from expert witness Peter Waite, was given that in producing the safety case, an argument must be constructed to give confidence that the operators had considered all the risks and that its principal purpose was to a tool, a route map and a record of commitments for management to set out how they organise their operation to work safely<sup>6</sup>.

In discussing the principles of permissioning regimes, the HSE note in a recent discussion document that the duty-holder must carry through the assertions and assumptions in the safety case to practices on the ground and monitor and evaluate their implementation<sup>7</sup>.

Overall the content of safety cases is common throughout the major hazard industries and can be summarised as:

- i) A descriptive section which provides plant and operations details, including design standards. This provides a demonstration that the facility was designed and built appropriately;

- ii) A description of safety management arrangements. This provides a demonstration that the facility is operated and maintained appropriately;
- iii) An assessment of the residual risks. This shows that the residual risks are as low as reasonably practicable;
- iv) Conclusions as to the adequacy of the safety based on i) to iii) above.

A report with these contents is likely to meet the requirements and suggestions discussed above.

### **SAFETY CHALLENGE FACED IN MAJOR INFRASTRUCTURE PROJECTS**

The construction of major infrastructure, such as transport links, utilities, airports or major building works and its subsequent operation and maintenance presents a range of major health and safety issues, which generally affect workers but can also impact on members of the public and the environment. Where the major hazard safety regulations don't apply – a wide range of health and safety legislation is in place from the Health and Safety at Work etc. Act through general safety regulations such as the Management of Health at Work Regulations, 1999 to specific design and construction requirements such as the Construction (Design and Management) Regulations 1994 and many others.

In addition to health and safety issues there are concerns over the practicality of options for the design such as can it be maintained, will it work, what emergency or standby provisions need to be in place, how much does it cost, how much will it cost to operate and what are the non-safety related risks with it such as business interruption and asset loss or damage in the event of plant or equipment failure.

In any major infrastructure project there are many parties involved or interested in the decision-making including:

- the final owners, who are likely to have business objectives to meet,
- operations teams, who will have to deal with any of the problems of operating the facility successfully,
- the designers/project managers, who are responsible for ensuring the right design for the right price and to programme.
- emergency services, who may be called in to provide fire and rescue activities,
- Maintainers, who may be third party maintenance contractors who need suitable and safe access and facilities,
- Other stakeholders which may include the public, government (national and local), environmental groups, etc.

The immediate requirements of these stakeholders may not necessarily be compatible with all of the requirements under the health and safety legislation and attempting achieve the right balance can be a source of conflict and ultimately cause delay, cost increases and in the worst case sub-standard levels of safety and environmental protection. Therefore the challenge is identifying, demonstrating and agreeing the best way forward in contentious areas where safety is an issue. The safety case was proposed as a way of meeting this challenge.

### **SAFETY CASE PROCESS ADOPTED FOR INFRASTRUCTURE PROJECTS**

A number of projects have been trialled by the authors using the safety case as a tool for aiding decision-making. The team creating the safety case included health and safety specialists experienced in producing safety cases in the high hazard industries as well as those with experience in CDM and the specific health and safety issues related to the construction industry. The team also included members of the design team who were looking at the various options involved.

### **PRODUCTION OF AN OPTIONS SAFETY CASE REPORT**

The first stage in our process was to identify where a safety case was required. Unlike the high hazard industries where a safety case is provided for an entire facility, the safety case approach was used to deal with specific issues raised for the facility. So for example, safe maintenance and access may have been identified as a concern with a number of possible options to deal with the problem. If there is no consensus on which option to use, the safety case can be specifically produced to deal with this issue.

Typically these issues were raised from risk workshops where the risk register was being reviewed or updated – or, where projects use them, from HAZOP studies.

The next stage in our process was to carry out a more detailed review of the hazards from the identified options. This typically involved face-to-face discussions with the interested parties, including operators and maintainers, the design team and many of the third parties. These meetings were intended to include staff at all levels – from the operatives who would carry out activities in the facility to Senior managers with business objectives to meet. In addition to these meetings, a series of interviews with experts in the particular area of concern were carried out. For example if the issue was related to confined space access, then suppliers of safety equipment and confined space rescue organisations were consulted.

From these meetings the hazards could be further developed and understood and the practicalities and effectiveness of using available safeguards, both hardware and managerial could be understood. With a better understanding of these, the options could be reviewed and amended.

The following stage required assessment of the options. This involved 3 elements:

- A review against codes and standards and the opinions of experts as to best practice. This included the hardware safeguards in place to control risks,
- A review of the management systems to see if the systems were in place to deal with operating and maintaining the options – or whether they could be put in place. This included the emergency arrangements that may be required,
- A review of the residual risks. This included documenting the hazards identified, some qualitative risk assessment and some quantitative risk assessment including cost benefit analysis and determination of whether risks were reduced to as low as reasonably practicable.

These 3 elements relate to the items i) to iii) noted earlier as the first 3 elements of the safety case. In carrying out the elements the review was intended to confirm or dispute that

an option was justifiable on health and safety grounds, i.e. that it met codes and best practice, that it could be managed safely and that risks were reduced to as low as reasonably practicable.

The results of these studies lend weight to a particular option being preferential. The next step was to return to the stakeholders and discuss the findings. From this, consensus could be gained as to the viable option.

Having gained agreement in principle from the interested parties on the way forward for the design, the Safety Case Report could now be constructed. Each of the 3 elements described above was documented. Additionally, detailed descriptions of the facility, its method of operation and maintenance and any emergency response required for hazardous situations. This additional information was included in order to define the “safe working envelope”, i.e. the limits of operation which were assessed and therefore to which the conclusions of the report apply. This is common to safety cases produced in the high hazard industries. A series of appendices were attached to the safety case including:

- the detailed reviews against codes, guidelines and regulations,
- proposals for 3rd party activities, such as maintenance programmes or emergency standby services (such as in the case of confined space emergency teams),
- minutes of meetings with all of the interested parties.

This last item is particularly important. The meetings with interested parties contained discussions of their agreements and the conditions by which they gave agreement. For example a maintenance team leader was happy to see a reduction in access points to a particular area, but only when it was explained that stairs would be provided at the access points rather than ladders.

The final element to the safety case was the conclusions – the justification of adequacy of safety. This included the conclusions that:

- the design option met relevant codes and standards, legislative requirements were met,
- the facility could be operated in the way described and that the arrangements under the management system in place by the operator was or would be sufficient to allow safe operation,
- the risks had been reduced to as low as reasonably practicable. The approach to this differed from project to project and included cost benefit analysis using the “value of lives saved” approach, an approach based on placing the risks in context of other risks faced by the project, or by comparison to other industrial activities. The method of selection of the risk criteria was based on discussion with the parties as to what they felt most useful in understanding risk.

Having produced a final report this had then to be represented to all of the interested parties to ensure they agreed with the scope, their concerns were covered and they agreed with the conclusion. Each party was then asked to sign off against the document and the design option could go ahead. The finalised report would then allow close-out of HAZOP actions or seen as a control measure in the risk register for the project.

#### FURTHER CHANGES TO THE DESIGN

In any major infrastructure project, as the design progresses so changes are proposed from agreed options. The safety case was used as a means of controlling the changes which may have an impact on health and safety. Each change was submitted to the safety case team who reviewed the assessments in the report and commented on the impact. At this stage, the minutes of meetings with parties became very important. The reasons for acceptance of the option could be reviewed and any impact noted. A recommendation was made on any option, either that it did not invalidate the conclusions of the study, in which case the report was revised in line with changes and circulated to interested parties for their sign-off, or that it did invalidate the conclusions, with an explanation of why, and that the option should not go ahead.

In keeping with the premise that a safety case is a route map, the additional analyses, even for options that are not recommended, were added as appendices to the report. This provides a record of subsequent decisions and provides evidence of the designer's duties to identify, assess and control hazards.

#### **BENEFITS OF THE APPROACH**

Where our safety case approach was adopted it was felt to be of significant benefit to the project. The benefits identified include:

- A documented compliance with appropriate standards, codes and regulatory requirements.
- The safety case report became a central repository for all documentation relating to the health and safety issues, and can provide a useful reference later in the design or during operation, maintenance or decommissioning.
- The safety case process provided a route to achieve consensus between the interested parties. As the arguments in the safety case were developed logically and systematically with conclusions drawn on the adequacy of safety, and as the parties helped to shape and develop the arguments, there was a much better management of conflict and delays were limited.
- The process of holding meetings with all interested parties at all levels allowed a degree of workforce involvement in the design and in health and safety. This was beneficial to the workforce as their participation in the discussions provided them with additional understanding of the hazards of the new facility, and was beneficial to the design as the views and opinions of those who would have to make the facility work safely were heard and acted upon.
- The Safety Case Report became a living document and a tool which could provide a baseline for safety against which changes to the design could be measured. When further changes were suggested later on (particularly cost-saving measures) a rapid evaluation of the impact on safety could be made and the change justified or prevented.
- The safety case process provided demonstration that the client and the designers had identified hazards, assessed risks and provide suitable controls and safeguards, and that risks had been reduced to as low as reasonably practicable.

## CONCLUSIONS

The majority of safety cases produced are in response to a requirement of specific major hazards health and safety regulations. However an approach which has been based on the already established principles of safety case production has been adapted for major infrastructure projects, particularly in areas where contentious decisions had to be made. The approach was used as it was anticipated that there would be programme and cost benefits as the systematic approach would provide reasoned arguments as to the most appropriate option.

Additional benefits included those which safety cases are known to provide such as providing a route map to the safety of the design, and a repository of information, but also included benefits such as consensus building and workforce involvement as a result of particular aspects of the approach used.

## REFERENCES

1. Control of Major Accident Regulations, 1999, *Statutory Instrument 1999/743*
2. Offshore Installations (Safety Case) Regulations, 1992, *Statutory Instrument 1992/2885*
3. Railway (Safety Case) Regulations, 1994, *Statutory Instrument 1994/237*
4. HSE, 2002, Nuclear Site Licence Conditions, [www.hse.gov.uk/nsd](http://www.hse.gov.uk/nsd).
5. K.Cassidy, 1989, Chapter 13 of Safety cases within the Control of Industrial Major Accident Hazards (CIMAH) Regulations, 1984. Edited by FP Lees and ML Ang. *Butterworth & Co. (Publishers) Ltd.*
6. Ladbroke Grove Rail Inquiry, Part 2 Report; The Rt. Hon. Lord Cullen PC. *HSE Books*. 2001.
7. HSE, 2000, Regulating Higher Hazards: Exploring the issues. *DDE 15*.
8. HSE, 2000, Reducing Risks, Protecting People. *DDE 11*.
9. P Bishop, R Bloomfield, 1998, A Methodology for Safety Case Development. *Safety Critical Systems Symposium, Birmingham, UK*.
10. TJ Britton, 1999, Examining Safety Reports and Evaluating Safety Management Systems. *European Conference - Seveso 2000, Athens, Greece*