Safety Cases

Dr Dmitri Zotov, MBE, PhD, MRAeS

Introduction

Safety Cases are not the bags of useful stuff you take onto an accident site, nor yet are they first-aid boxes. They are a way of managing the safety of operations which can have a profound effect on the way regulations are written, or safety recommendations are made. In the same way that you may need to know the workings of an Electronic Flight Bag if you are investigating a take-off accident, knowing your way around a Safety Case may be necessary if you're looking into corporate failure.

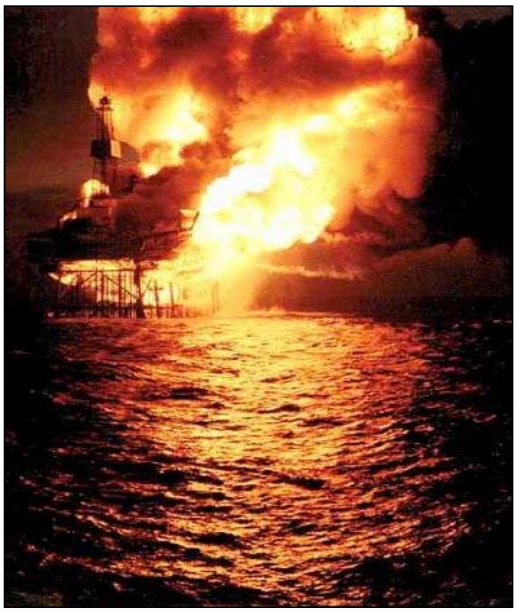
The term 'Safety Case' comes from the legal origin of the idea. In an inquiry into occupational safety and health, it was said that compliance with Regulations was not sufficient to ensure safety: it was necessary for the operator to 'make a case' that the system was safe to operate (Robens 1972). This meant, to demonstrate that it was safe, by producing evidence to support arguments that safe operation would be achieved.

Safety Cases are now required in hazardous industries such as offshore oil. They are not yet widely mandated in aviation, but there are operators who have recognised the benefits of using them, without a regulatory requirement. There is an increasing likelihood that you will encounter one in the course of an investigation: since an accident is a demonstration that the Safety Case has failed in some way, actions to avert a recurrence can include finding the deficiencies in the Safety Case.

History of Safety Cases

Piper Alpha

The destruction of the Piper Alpha oil rig in the North Sea was not the origin of Safety Case requirements, but it produced a huge boost to the general introduction of Safety Cases in hazardous industries.



The Commission of Inquiry commented that

Compliance with detailed prescriptive Regulations was not sufficient to ensure safety (Cullen 1990).

For example, the initial conflagration could have been nipped in the bud if the water deluge system had been effective. The Regulations required that the whole

of the production deck be covered by water spray. There was a physical limit to the amount of water that could be pumped from the sea to that height, and in order to assure complete coverage, relatively fine nozzles were necessary. These routinely became blocked by the corrosive action of sea water. At inspections, these blockages were noted and rectified, but inevitably others would become blocked by the next inspection.

In reality, there were only a few areas which needed to be drenched: much of the area could not sustain a fire. Had the Company been able to select only the relevant areas for coverage, much larger nozzles could have been used which would not have been subject to blockage. Additionally, the focussing of the available volume of water where it mattered would have been much more effective. In short, the apparently sensible Regulation was counter-productive.

A Safety Case, on the other hand, could and should be 'owned' by the operators, and so could be tailored to get the best results in their particular circumstances. Formal analysis of relevant hazards is required. Today, in Australia as elsewhere, offshore oil installations are required to be operated to a Safety Case. This is generated at the design stage, and the initial hazard identification and analysis is used to modify the design.

Are They Effective?

Error! Objects cannot be created from editing field codes.
Figure 1. Return on Investment: North Sea Oil,

Since the introduction of the Safety Case regime for North Sea oil, the previously recurring major accidents have ceased.

When Safety Cases were required, after the Piper Alpha disaster, they had to be produced from scratch: there were no safety systems as such. They cost significant sums, and the engineering work required to make good the deficiencies revealed cost a great deal more. However, the saving in terms of accidents which would have been expected on a historical basis (estimated by Det Norske Veritas) was more than twice the total cost – see Figure 1. (Pitblado and Smith 2000). These figures represent the insured cost: Wood (1997) estimates that the uninsured costs in airlines may be six times higher – lost revenue, disrupted schedules, and so on.

Clapham Junction

Generally, Safety Cases have been forced on industries after a major disaster. This picture is of

the Clapham Junction disaster near London, which arose from the failure of one signal. That in turn resulted from a deficient but probably widespread work practice. Such disasters inevitably result in a Public Inquiry, and the result has been recommendations for a Safety Case regime in that industry (Hidden 1989). These have then been enacted by Parliament. Wouldn't it be nice if the aviation industry could get in first, and pre-empt a disaster?

This could come about in two ways:

- a demonstration of the ways in which a minor accident could have been averted by a Safety Case, showing its potential to avert a major disaster, and
- showing how the collection of recommendations from an investigation could fit into a Safety Case regime, with wider benefits than conventional recommendations could achieve.

There may be potential problems with instituting a Safety Case regime:

- Cost – Preparing a Safety case can be a significant task. This applies to both the industry, and to the regulator, who must analyse the Safety Cases presented by operators.
- Ownership – A Safety Case is not something which can be bought from consultants, and left on the shelf to gather ticks at audit. It needs to be 'owned' by the company, who need to implement the measures described in it, and update it in the light of experience or when operations change. So, in an operation which is sufficiently complex to require a comprehensive Safety Case, the company will need to employ suitably qualified staff.
- Competency – Producing and analysing a Safety Case for a larger operator requires competencies not likely to be found among existing staff. Fortunately, the simpler Safety Case needed for a small operator would not require this depth of analysis, as will be discussed later.
- Move to non-prescriptive regulations – While adoption of a Safety Case regime is part of a move toward goal-setting regulations, in the past this has sometimes become a complete abandonment of prescriptive regulations. This has not been satisfactory: the need for some degree of prescription remains. For example, the requirement to fly with a line-feature on the left could not come from a Safety Case, but it is necessary in order to avoid collisions in VFR flight.

None of these difficulties is insuperable. The potential effectiveness od a Safety Case regime in averting accidents can be demonstrated in accident investigations, though this would need a greater depth of analysis than is usual at present. The cost of producing a Safety Case is trivial in comparison with the cost of an accident.

The larger operators who need a comprehensive Safety Case can afford the necessary specialist staff, especially in view of the Return on Investment.

Achieving a proper balance between prescriptive and goal-setting regulations is no more than an extension of existing regulatory processes.

Safety Cases in Aviation

Safety Cases in aviation are not exactly new, but until recently they have been part Safety Cases, rather than 'whole of operation'. For example, Eurocontrol produced a Safety Case for the introduction of Reduced Vertical Separation Minima (Eurocontrol 2001), and the UK CAA requires a Safety Case if an airline is planning to do something radically different from its normal operations.

One reason why Safety Cases are not yet widespread in aviation may be this confusion of nomenclature. You may hear 'Oh, we've got a Safety Case', when what is meant is some form of change management; a part Safety Case at best.

Partly, at least, the slow introduction of Safety Cases is due to the absence of formal inquiries, no doubt because Governments have shown trust in the official investigators. In other industries, Safety Cases have been the outcome of formal inquiries – Piper Alpha, Clapham Junction, Longford and so on. But in aviation, the last major inquiry has been the Moshansky inquiry into the accident at Dryden, Ontario (Moshansky 1992). This was contemporary with Piper Alpha, and although the existing regulations were demonstrably ineffective in averting the accident, Moshansky did not look at the potential for a Safety Case regime.

Another reason is that regulators haven't mandated them. SMS has been increasingly promoted as the answer to the maiden's prayer. An SMS is necessary, but it is not sufficient. Think of the analogy between a business plan and a Financial Management System, on the one hand, and a Safety Case and a SMS on the other. A FMS may tell you to the last cent how money has been spent, but without a business plan you won't know whether it has been spent to best advantage. In exactly the same way, without a Safety Case, you will have no real idea how effective your safety efforts have been, nor whether you have done everything necessary to assure safe operation. *A SMS is part of a Safety Case*.

However, the limited application of Safety Cases in aviation is changing:

- Eurocontrol is producing a draft Safety Case manual.
- The UK CAA explored the practicality of goal-based safety regulation in 2001, and now requires Safety Cases for aerodromes and ATS providers. It is considering requiring Safety Cases for maintenance and flight operations.
- The FAA now issues guidance on Safety Cases for airworthiness standards, which has been followed by the Australian Defence force.
- In Australia, CASA is using a Safety Case approach to the National Airspace System; Air Services Australia uses it for new developments such as RVSM.

You can see the increasing likelihood that an investigation will encounter a Safety Case. For example, if you are investigating a TCAS incident in upper airspace in Australia, involving RVSM, that is what you will find.

Accident Investigation

So where do accident investigators fit into the picture?

These days we go well beyond finding the immediate facts of an accident. At least in Air Transport accidents, we look for the underlying hazards and the corporate factors which give rise to them. We will want to know whether the hazardous conditions were known beforehand, what was done about them, and why actions may have been ineffective. We need to look at factors such as communications within the company, and whether these were impeded by the company structure. As we shall see, this amounts to examining the validity of the Safety Case. This is so whether or not there is a formal Safety Case in place.

Also, we may find that our Safety Recommendations can have more general application, if they are couched in terms of how the Safety Case should be designed and tested, rather than as actions by an individual operator.

In the Ansett case study which was presented at Queenstown (Zotov, Hunt et al. 2005), analysis with the Theory of Constraints isolated a few core problems, but a surprisingly large number of recommendations were needed to address them. However, *all* of the recommendations in respect of the airline – having a Safety Department, lines of communication and so on – could be distilled into

"Airlines should be compelled to operate within a Safety Case".

Having a Safety Case would prevent the abolition of the Safety Department, since this would invalidate the Safety Case and ground the airline; resourcing of the Safety Department would have to be addressed in order that it could perform its required functions within the Safety Case; monitoring of recurring defects would have been addressed during the hazard analysis; and so on.

Safety Case Definition and Structure

What is a Safety Case? :

- "A documented body of evidence that provides a demonstrable and valid argument that a system or equipment is tolerably safe for use: within a defined envelope, throughout the proposed life of the equipment". (UK MoD JSP 430).

The UK Ministry of Defence, like the Australian Defence Force, now operates (in part) within a Safety Case regime. And it never uses one word where five will do! Setting aside the verbiage, it means

"The body of evidence that the system is safe, together with the argument that makes sense of the evidence."

There is no point in building up a large volume of documentary evidence, which you allege shows that the system is safe, without telling readers what all this evidence means, and showing *how* it proves the system to be safe.

Notice that there is no reference to Regulatory compliance.

Structure of a Safety Case

The Safety Case comprises two parts:

- The Safety Case Report – the body of evidence that the system will operate safely, and the argument that makes sense of it – and
- The SMS that implements the Safety Case Report.

See Figure 2.

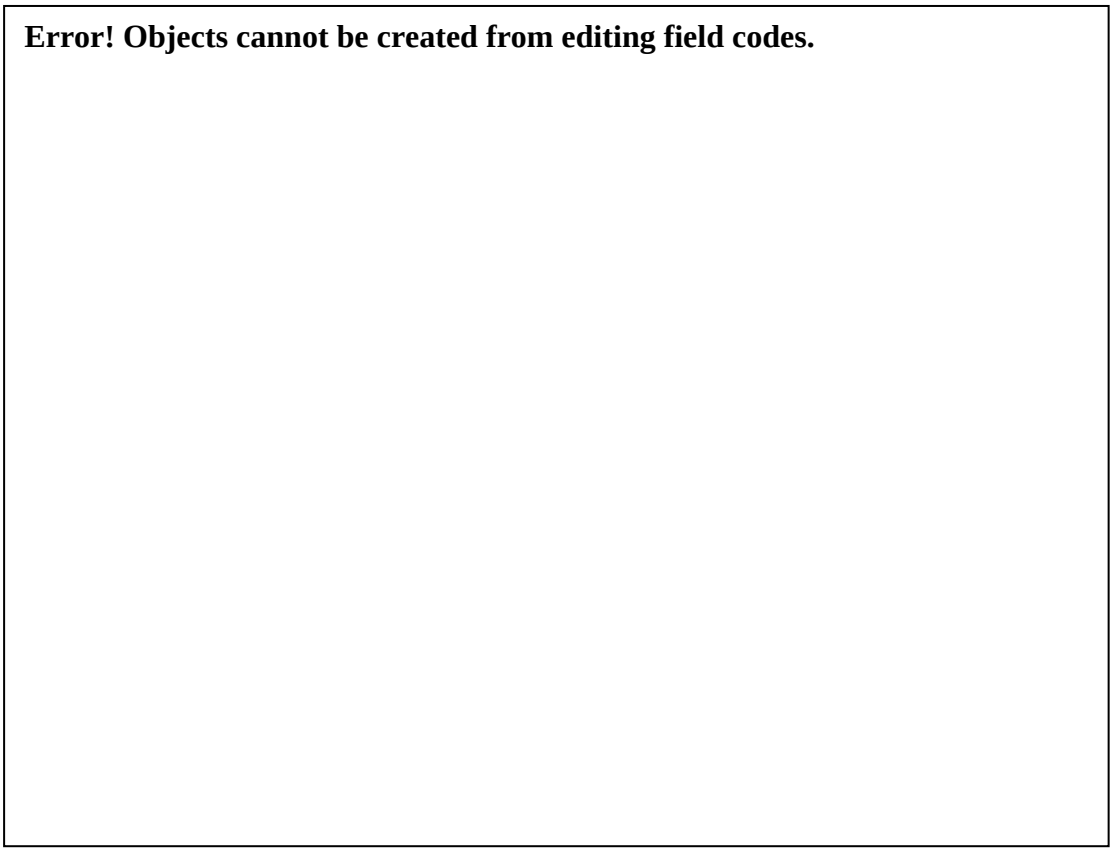


Figure 2. Structure of a Safety Case

The Safety Case Report documents all the things which will be done to assure safety, *and* the supporting argument proving that these things will assure an acceptable level of safety.

The SMS comprises those things you need to comply with your Safety Case – the Safety Manager, Safety Committee, and so on. Its function is to compile the Safety

Case Report, and through-life management of the Safety Case, with appropriate reviews and audits.

In reality, there are some arrows going the other way, but not shown, for clarity. We mentioned the loop from the SMS, back through Safety Case production, for example.

The Safety Case Report says *what* will be done, the SMS is about *how* it will be done.

Expositions and (current) Safety Management Systems are associated ideas which can fit into the Safety Case concept.

Exposition is a term used by the NZCAA, and by EASA (Maintenance regulations only). It means a document which demonstrates that the company complies with the Regulations, and details the company structure, and the procedures it will follow. The underlying assumption is that compliance with the Regulations will assure safety. The further assumptions are:

- that the Regulations are absolutely complete: nothing else needs to be done to assure safety
- that the Regulations are absolutely clear – there is no room for misinterpretation, as happened in the Glenbrook rail accident
- that it is possible for everybody to know the detail of all the Regulations that affect them – how else can they be expected to comply?

What about an SMS without a Safety Case, as we now have? Such a Safety Management System seeks to identify hazards and drive them down. The underlying assumption is that this activity, together with regulatory compliance, will assure safety.

These various ideas are, of course, inter-related. We can see that the functions of a stand-alone SMS map to some of the Safety Case functions. Other functions map across from the Exposition. (See Figure 3).

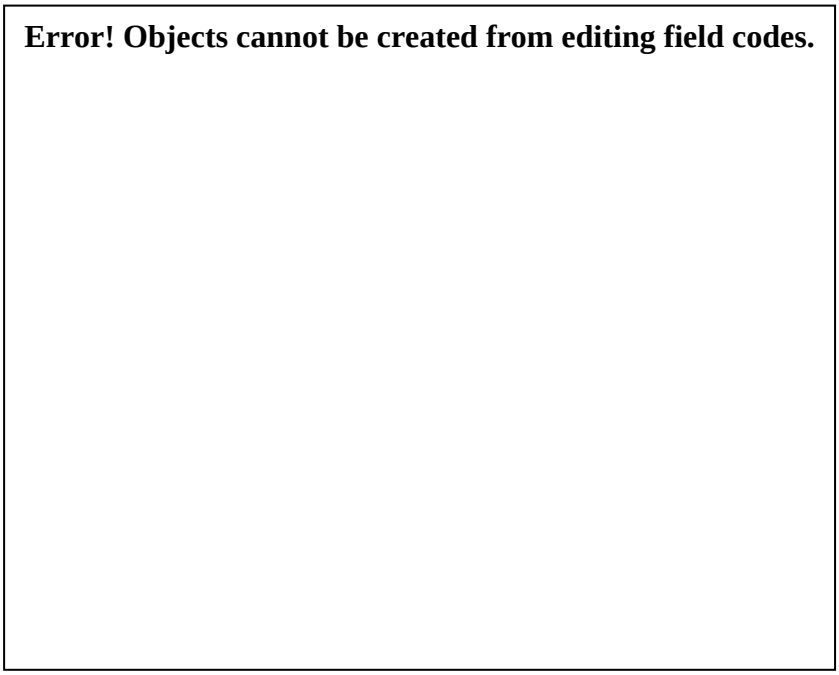


Figure 3. Relationships between Safety Case, Exposition and SMS

What neither SMS nor Exposition contains, however, is the self-contained evidence and supporting argument that enough has been done to achieve an acceptable level of safety. So, while both Expositions and SMSs can give improvements over what we had before, to get the full benefit we need to introduce Safety Cases – which is why they're becoming widespread.

Examination of a Safety Case

How would you go about examining a Safety Case after an accident? Essentially, you will need to backtrack through the processes which should have been used to generate it in the first place:

- Was the evidence that the system would operate safely, gathered and documented?
- Does the argument show why what has been done will result in a system that will be acceptably safe?
- Has the SMS been formed and documented?
- Have risk assessments been performed – and acted on, if need be?

Error! Objects cannot be created from editing field codes.
Figure 4. Safety Assessment Techniques

Safety assessment uses a range of methods for hazard identification, which may be new to investigators. In fact, this level of analysis will probably require you to add some tools to your bag. Naturally, you don't have to be an expert in component failure analysis, any more than you have to be an expert metallurgist: your expertise involves knowing when you need an expert, and in understanding what he's saying. Techniques range from direct observation to component failure analysis; estimation of likely consequences (essentially, expert judgement) and frequency estimation (generally open to quantitative analysis) and consideration of criticality and ALARP.

Error! Objects cannot be created from editing field codes.
Figure 5: As Low As Reasonably Practicable

ALARP – the "As Low As Reasonably Practicable" principle (Figure 5), is required by law (Edwards v National Coal Board, 1949). Some hazards are so bad that, if they cannot be modified, the operation must stop. (For

example, critical metal fatigue). Others are so remote (or inconsequential) that they may safely be ignored. In between comes the range where hazards are not too bad, but could be reduced further. It is not open to managers to 'accept' such risks, as they might decide to do with commercial risks. Safety risks must be driven down until they are ALARP; that is to say, they must be reduced until the cost of any further improvement is entirely disproportionate to the improvement in safety. You need to be able to determine whether ALARP has been achieved. But how should the boundaries be set?

There have been two approaches:

- British Rail distinguishes between
  - large operators, such as mainline expresses, which must do full quantitative assessments of risk and hazard, and
  - Small operators, such as vintage rail societies, where a purely qualitative approach is considered sufficient. For example, a vintage steam locomotive might be driven exclusively by experienced (and not youthful) enthusiasts who are not given to irresponsible behaviour; it might operate only on branch lines at 30 km/hour. It might be accepted that sufficient hazard reduction, on approaching a level crossing, would be achieved by blowing the whistle twice.

  The British Rail approach could be a good approach in aviation, given the wide range of operators in terms of size, resources and capabilities.

- Eurocontrol has set quantitative levels, following a lengthy study by Det Norske Veritas (Spounge 1998):
  - The intolerable level is set at 2 x Target Level of Safety
  - The acceptable level is set at 0.02 x TLS

  This seems a sound approach wherever there is an accepted TLS. In air transport operations, this is typically set at something like 1: 10^7 hours of operation. Based on the Eurocontrol study, these bounds should be defensible. This method would be suitable for large operators like Air Services Australia and Qantas.

Error! Objects cannot be created from editing field codes.

A Safety Case needs to be pragmatic. The object is not to generate wallpaper. The Safety Case should be matched to the size and complexity of the operation. This small aircraft (Figure 6) requires only a simple Safety Case (Figure 7).

Figure 6: A simple operation

- It is built to a quality standard, so small parts which might be harmful to the user are unlikely to break off.
- But should they do so, we restrict users to three years of age or older, who are unlikely to swallow small parts.
- Should they nevertheless do so, we have a contingency plan.

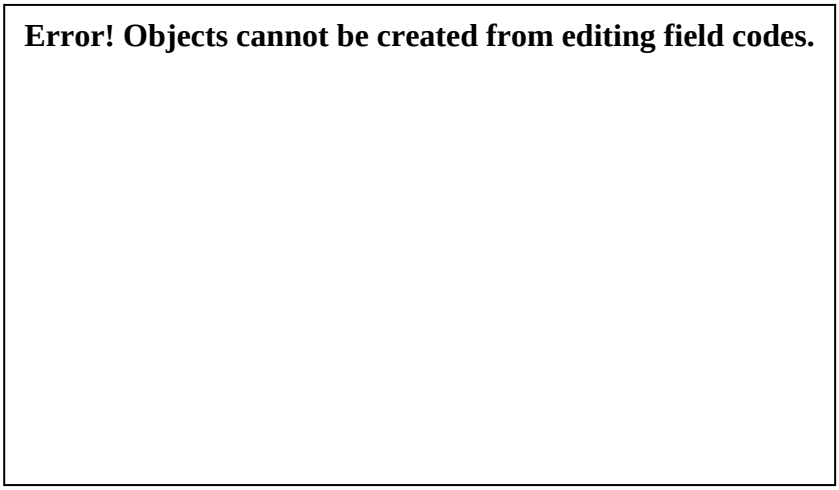


Figure 7: A Simple Safety Case

The SMS isn't shown, but it is Mum, who ensures that the two-year-old does not snitch the three-year-old's toy.
This Safety Case meets all the requirements of the Defence Standard.

Summary

The use of a Safety Case to prove that an operation is acceptably safe is now recognised as world's best practice, and is being progressively mandated in various hazardous industries.

In the event of an accident, examining the Safety Case can give clues to what has not been done properly, at corporate level.

Safety Recommendations framed in terms of modifying a Safety Case can have generic application.

References:

EN.REFLIST