Safety Management in Complex Engineering and High Hazard Environments - A Personal Perspective

If you think Safety Management is expensive then try having an accident

Introduction

This is a personal perspective on the management of Safety in complex and high hazard industries and operations. In the text I will refer to and comment on many aspects of safety management, it's history, it's legislation and the implications for those involved. The treatment is from a UK perspective, but I will use one case and one example from the USA. Before continuing I will post a disclaimer; this is not a peer reviewed and referenced academic paper, it is a personal perspective from a practicing safety professional and a Duty Holder. However, within the text you will see key words and phrases that you can use to search peer reviewed papers, and of course the numerous Public Inquiries that have stemmed from the most severe accidents, I include a list of relevant Public Inquiries as it is always better to learn from other's mistakes rather than your own. Real examples will be used throughout the text, but names may be altered or omitted. This article is intended to be thought and debate provoking.

Why Manage Safety?

The Deepwater Horizon Platform

There are numerous reasons why safety of products, services and operations should be rigorously managed; these range from legislation, the fear of prosecution, moral judgement, protection of reputation and brand or enterprise value, or just good business sense. There is also a cost to not doing it well; an anonymous, but oft quoted saying is "if you think managing safety is expensive then try having an accident". I think the owners and operators of the Aberfan Works, the Flixborough Plant, the Herald of Free Enterprise, Piper Alpha, the Railway at Ladbroke Grove, the Deepwater Horizon platform, and Nimrod FV230 would agree with this anonymous commentator. The cost is not just monetary, it must also be measured in terms of lost brand value and destroyed reputations and the painful loss of the casualties and their families and also, potentially, capabilities that the health, wealth or defence of the Nation depends.

Who is responsible for Safety?

The Flixborough Plant

It is useful to explore exactly who is responsible for safety and the bounds of this responsibility. As with all things legal, this is not clear cut and has evolved through various judicial rulings, case law and Public Enquiries. The Health and Safety at Work Act

(introduced in 1974 in the UK) is wide ranging in its definitions of who has a duty of care for others. The author's lay interpretation is that everybody has a duty of care for everybody else and can be held responsible for their actions, and just as importantly, their omissions. That said, some parties, namely employers, are likely to have greater opportunity to act, or omit in a manner to build or undermine safety.

Irrespective of whether everybody has a duty of care or not, there will be some individuals within an enterprise who by their position or influence or designation, have a much greater sway in the management of safety than others. I will term these Duty Holders and these individuals are the "controlling minds" that prosecutors seek to identify if a situation comes to court. I have found no strict definition of a Duty Holder; the interpretation can vary with industry and with context, however, the definition can probably be bounded by; Owner or Operator, Creator or Controller of Risks. A working definition could be "if you are the person who has the position or influence to create actions or omissions that materially affect risks to the safety of any party owed a duty of care" then you are a duty holder and if there is a serious accident then you can expect to stand trial in a criminal court. The Health and Safety Executive is itself not entirely clear stating "ultimately it is for Courts to decide whether or not duty-holders have complied with the law". The Authority of Duty Holding can be delegated, but not the Responsibility. If you delegate then you remain responsible for the actions and omissions of the delegate.

The terms duty holder and Duty Holder are sometimes used interchangeably, but can be distinct. Some organisations seek to deconflict the similarity of terminology by using different titles such as Technical Authority (TA) or Approving Authority (AA) or even Technical Approving Authority (TAA). It is the author's view that the title is secondary, the primary consideration must be clarity in responsibility and in the boundaries of that responsibility and how information and decisions are communicated across the boundary (see the next section where the terms "safe to operate" and "operate safely" are introduced).

This does not mean that only the designated Duty Holders are responsible for their actions or omissions. Any organisation will have people in positions of authority who may consciously or unconsciously influence safety related matters and who may have objectives and priorities very different from the Duty Holder. This can give rise to tensions and to difficult decisions. In the author's experience, a simple reminder that the actions being proposed have a direct impact on safety and if implemented will put the person promoting that course of action in the position of the controlling mind, serves to clarify the situation. However, this must not be used as an easy route to influencing a decision; the role of Duty Holder is a responsible one and must not be abused. But what about when these external safety related decisions happen in spite of the cautions expressed? Well, the Duty Holder has some difficult decisions to make, rescinding the position is an option, but it really is an abdication of responsibility, not an exercise of responsibility. What is absolutely clear is that taking no action is the worst response. This is an area where the independent expert, or the second opinion can be valuable. Of course there is the option of the Duty Holder exerting their authority as well, to stop an operation or to remove a system or equipment from service, pending safety investigations can be the right and responsible action, although this could be draconian. Other options include taking actions in the full knowledge of the system and its environment and to place limits on operation, reducing the operational envelope or imposing environmental constraints such as temperature, pressure or speed. The author has used this when the emergence of material quality issues indicated that operating below 0˚C could cause a

catastrophic brittle fracture in an important system. The interim solution before correctly specified components could be installed was a temperature and sea state limitation, and, if the constant tension device was not operating, a more severe sea state limitation, the result - the Royal Navy (RN) retained capability in an acceptably safe manner.

Is this Complicated or Simple?

The management of safety must be as simple as practicable, clear lines of sight from design, through manufacture into operations, maintenance and modifications. Governance must be simple with decision making by persons close enough to the product or operations to understand the detail and sufficiently senior to have clout. Easily stated, but more difficult to put into practice.

The clarity, the lines of sight, must cross organisational boundaries and communications must be clear and simple and the responsibilities of all stakeholders be apparent to all. The management of ship safety in the MoD has a simple phrase, the acquisition and support organisation provides the RN with ships "safe to operate" and the RN "operates ships safely" - the high level responsibilities are abundantly clear.

The Herald of Free Enterprise

Rules, Regulations, Standards and Safety Cases

So far the text has been about governance, management and responsibilities. Now it is necessary to introduce some practical Safety Management. It may be easy or convenient to assume that if a standard is met then safety is sufficiently covered. There could be an argument in favour of this, but a crude application of standards is limited in its effectiveness. The Ford Motor Company in the infamous Pinto saga met all applicable standards, yet, in an era when the lessons of Ralph Nader's "Unsafe at any Speed" had not yet embedded and in accordance with standards, Ford produced a car that would suffer fuel tank rupture and fire in collisions. Indeed, every crash test conducted confirmed this. Ford were prosecuted and suffered punitive damages, not for ignoring standards, but for callously putting a cost to life, and based on this not even implementing the most inexpensive of modifications. That said, putting a price to life is not wrong, but today (see UK Health and Safety Executive guidance), the concept of Gross Disproportionality has been introduced and the use of a value of life is intended to guide where safety money is best spent, not for avoiding expenditure. This value based approach is useful where an ALARP (As Low As Reasonably Practicable) case is being made, but it does not work where safety is clearly unacceptable.

Standards must be appropriate and current and fit for the environment, and even then are not infallible. Many rules and standards are evolutionary in their development, capturing and coding hard won experience and learning from past accidents and incidents, and as such are limited. A good example of such a limitation, from the author's experience, was in the production of submarine escape breathing equipment. The standard was clear and

the manufacturer applied the standard. However, when the manufacturer was changed costly and dangerous failures occurred. Investigations showed the standards were still being met. The issue was the original manufacturer had always exceeded the standard and in the particular application that was critical, the standard was insufficient for the environment!

This brings us to the Safety Case, a reasoned, auditable, comprehensive and documented body of evidence that provides a compelling argument for the safety of the equipment, system or plant in its operating environment, covering normal, emergency and damaged situations. Useful, perhaps essential, for the assurance of safety in any complex situation. The objective of the case is to provide assurance that safety is ideally, "broadly acceptable", at least "ALARP" and not "unacceptable" (see the previous section on the value of life).

Before a safety case is started, the organisation must be clear on its safety expectations. These may be industry or societal standards, but the organisational or social expectations may be difficult to determine. In a previous article on risk management the author used the example of differences in risk appetite between manned space flight and neonatal care. Another example could be the different stages of an aircraft development, a different standard of safety may be acceptable in the development phases with test pilots who are skilled and understand the risks versus the service phase with widened areas of operation and a broader range of pilot skills and with different impacts arising from an accident; both situations will require a Safety Case. Of course there are anomalies, just look at transport and the gulf in what appears to be socially acceptable between air, rail, car and motorcycle travel.

The material for the Safety Case body of evidence can be wide and varied; Standards do have a part to play, as long as their use (or decision not to use) can be objectively justified, other elements of evidence can include calculation, modelling, simulation, test and trials data and in-service feedback; Failure Modes Effects and Criticality Analysis, Fault Trees Or Bow Tie diagrams. The Safety Case must include underpinning assumptions and limitations and these must be accurately recorded. With any assumptions it is important to regularly test them; for instance, the safety of a plant may in part be based on the presence of a suitably trained crew; does the operator's training pipeline maintain or enhance historical standards?

The Safety Case is not static and should be revisited if there are material changes in the equipment, modification status or the operating environment. This can become difficult to assure unless there are processes in place to govern many aspects of ownership. The

Nimrod FV230 Fatalities

cases must also stay in touch with reality; it is relatively easy to complete or update a paper exercise, but what is the situation on the ground, what is the material state of the plant? Material State assessments can be useful in maintaining the link with reality and informing the Safety Case.

The Safety Case must be clear in its scope and its bounds and the type of failures considered; these could be related to the intrinsic safety or the functional failure effects. An example may be in the assessment of a high pressure bilge or ballast pump for a

submarine. The pump and its associated control equipment may be demonstrably safe in terms of intrinsic hazards, electrical, mechanical, control; but, if the pump fails to provide the correct head and flow when required the submarine could be lost. This is a lesson the United States Navy learned the hard way with the USS Threasher, minor pipe work failures led to the reactor automatically and irreversibly shutting down, just when reactor power was needed, a unrecoverable depth excursion and lost submarine was the result.

Some Challenges

In previous sections, the importance of communications, clarity in evidence and decision making and timely collection of evidence has been stressed. There are practical challenges to this, especially across organisational boundaries; clear contracts or other agreements can be useful, but personal relationships are equally, if not more so in keeping clear, concise and accurate information flowing. The author is reminded here of an example of where there were serious concerns over the safety of complicated and operationally essential equipment fitted to most RN ships. He, as Duty Holder, was chairing a SQEP (Suitably Qualified and Experienced Personnel) panel, a group of around 20 people representing the user, other Duty Holders, materials and engineering experts, the OEM, the subcontractors, the regulator and a third party assurer. When asked the question "should this capability be removed from service", the OEM, subcontractors and

Ladbroke Grove Rail Accident

assurer all said "yes immediately", indeed one of them said "we have done some independent analysis and our lawyers advise that we share no information with you". Why did these parties behave in this manner? It is clear that they had nothing to gain from taking any risk and could only lose if their past failings came to light (all the problems of the equipment was from their failings). The author's response? He dismissed all those parties and continued the panel with independent expertise and those with a legitimate interest in safety of operations. The result? The equipment was kept in service, with a reduced operating envelope and an enhanced inspection regime until modifications could be completed - safety was assured and operations continued.

The Safety Management System

The previous sections have talked about wide and varied topics, Governance, Duty Holders, Safety Cases, communication, transparency, legislation, regulations, standards, training, the list is long. What has not been mentioned is how all these things are related and coordinated. This is where an Organisation should have and maintain a Safety Management System (SMS). In short this is a formal framework to manage all aspects related to safety and will include; risk identification, safety targets, governance, reporting processes, audit processes, investigation processes, training and the assurance of SQEP (Suitably Qualified and Experienced Personnel). For transient activities such as a project, a full SMS may not be justified and the use of a Statement of the Organisation and Arrangements (O&A)for safety may be acceptable. The author's view is that if an O&A is used it must have a stated life and include arrangements for integration into the wider organisations SMS.

Conclusions

This document is intended to introduce some personal experiences of Safety Management and to introduce some ideas and some lessons from history. As a thought provoking paper, the conclusions should come from the reader as much as the author, but some will be stated:

Safety must never be ignored.

Safety is dynamic and a Safety Case is a useful technique for maintaining a current body of evidence for assurance.

Accidents are expensive in every respect.

Everybody has a duty of care, but for some this duty will be larger.

The Duty Holder is responsible and must act as such, be clear in their authority, and exercise it objectively, not being swayed by misinformation, politics, vacillation or vested interests.

And not mentioned in the text, Professor Reason's "Swiss Cheese" model is very useful in visualising layers and holes in safety protection.

Debris from the USS Threasher

References:

A. Haddon-Cave, The Nimrod Review: an independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006. Report dated 2009, ISBN 9780102962659.

B. Cullen, The Ladbroke Grove Rail Inquiry Report, 2001, ISBN 0717620565.

C. Cullen, The Public Inquiry into the Piper Alpha Disaster, Report Dated 1990, HMSO, ISBN 0101113102.

D. Sheen, MV Herald of Free Enterprise report of court No. 8074, Formal Investigation, 1987, ISBN 0115508287.

E. Parker, Formal Investigation into Accident on 1 June 1974 at the Nypo Factory at Flixborough, 1975, ISBN 0113610750.