Lessons from Esso's Gas Plant Explosion at Longford

Andrew Hopkins PhD
Australian National University
email:andrew.hopkins@anu.edu.au

In September 1998 Esso Australia's gas plant at Longford in Victoria suffered a major fire. Two men were killed and the state's gas supply was severed for two weeks, causing chaos in Victorian industry and considerable hardship in homes which were dependent on gas.

What happened was that a warm liquid system (known as the "lean oil" system) failed, allowing a metal heat exchanger to become intensely cold and therefore brittle. When operators tried to reintroduce warm lean oil, the vessel fractured and released a large quantity of gas which found an ignition source and exploded.

In what follows I shall trace the reasons for this event, relying on evidence provided to the Royal Commission which investigated the disaster. (For further details see Hopkins, 2000).

Operator error?

There is often an attempt to blame major accidents on operator error. This was the position taken by Esso at the Royal Commission. The company argued that operators and their supervisors on duty at the time should have known that the attempt to reintroduce a warm liquid could result in brittle fracture. The company claimed that operators had been trained to be aware of the problem and Esso even produced the training records of one operator in an attempt to show that he should have known better. However, the Commission took the view that the fact that none of those on duty at the time understood just how dangerous the situation was, which indicated a systematic training failure. Not even the plant manager, who was away from the plant at the time of the incident, understood the dangers of cold metal embrittlement. (Dawson, 1999:197). The Commission concluded that inadequate training of operators and supervisors was the "real cause" of the accident (Dawson, 1999:234). It is clear therefore that operator error does not adequately account for the Longford incident. This is a general finding of all inquiries into major accidents (Reason, 1997).

Although the Commission spoke of inadequate training as the "real cause", we are entitled to ask: "Why was the training so inadequate?" or more generally "Why were the operators and their managers so ignorant of the dangers?" And as soon as we ask these questions, a host of other contributory factors come into view. We need to uncover these more fundamental causes in order to identify the real lessons of Longford.

The failure to identify hazards

A major contributing factor was the fact that Esso had not carried out a critical hazard identification process, standard in the industry, know as a HAZOP (short for hazard and operability study, see Bahr, 1997). This procedure involves systematically imagining everything that might go wrong in a processing plant and developing procedures or

engineering solutions to avoid these potential problem. HAZOPs had been carried out on two of the three gas plants at the Longford refinery but not at gas plant one, the oldest of the three. A proposed HAZOP of this plant had been deferred indefinitely because of resourcing constraints. By all accounts a HAZOP would have identified the possibility of cold temperature embrittlement caused by a failure of the lean oil system. Even Esso's parent company, Exxon, acknowledged that the failure to carry out this HAZOP was a contributing factor to the accident. The failure to identify this hazard meant that operating instructions made no mention of what to do in the event of lean oil failure and the result was that operators neither appreciated the seriousness of the problem when it arose nor knew how to handle it. In short, inadequate training was a consequence of inadequate attention by the company to hazard identification.

The failure of the Safety Management System Audits

The Royal Commission severely criticized Esso's safety management system (OIMS) and the auditing of that system. "OIMS, together with all the supporting manuals, comprised a complex management system. It was repetitive, circular, and contained unnecessary cross-referencing. Much of its language was impenetrable" (Dawson, 1999:200). As for the auditing of the system, Esso had conducted a major audit of OIMS less than a year before explosion. This audit failed to identify any of the problems which gave rise to the explosion, and in particular, failed to uncover the fact that the critical hazard identification process had not been carried out. The Royal Commission states that "it can only conclude that the methodology employed by the assessment team was flawed"(Dawson, 1999:199).

The failure of audits to identify problems revealed in post-disaster inquiries is unfortunately commonplace. Following the fire on the Piper Alpha oil platform in the North Sea in 1987, in which 167 men died, the official inquiry found numerous defects in the safety management system which had not been picked up in company auditing. There had been plenty of auditing, but as Appleton, one of the assessors on the inquiry, said "it was not the right quality as otherwise it would have picked up beforehand many of the deficiencies which emerged in the inquiry" (1994:182). In fact audits on Piper Alpha regularly conveyed the message to senior management that all was well. In the widely available video of a lecture on the Piper Alpha disaster Appleton makes the following comment:

> When we asked senior management why they didn't know about the many failings uncovered by the inquiry, one of them said: "I knew everything was all right because I never got any reports of things being wrong". In my experience , ... there is always news on safety and some of it will be bad news. Continuous good news - you worry. (ICI video recording of a lecture by Appleton)

Appleton's comment is a restatement of the well know problem that bad news does not travel easily up the corporate hierarchy. High quality auditing must find ways to overcome this problem.

Esso's managing director reported to the inquiry that the Esso audit had shown that most elements of the safety management system were functioning at level three or better. "(Several

elements of the safety system) were assessed at level 4, the highest assessment level", he said. He noted also that an internal review in May 1998, 4 months before the explosion, "highlighted a number of positive results", among them, six months without any recordable injuries... high levels of near miss reporting .. and major risk reduction projects." (T5455).

This was clearly the "continuous good news" which Appleton had said was a cause for concern. It indicated that Esso's auditing was not of sufficient quality.

The failure of Esso's incident reporting system

There were numerous warning signs that things were going wrong at Longford. For instance, hours before the incident, ice was visible on piping which was normally too hot to touch. This was a direct precursor to the accident but the full significance of the anomaly was not recognised and there was no effective response. A similar cold temperature incident a month earlier had been allowed to pass without an investigation.

Ironically Esso's safety performance at the time, as measured by its Lost Time Injury Frequency Rate, was enviable. The previous year, 1997, had passed without a single lost time injury and Esso Australia had won an industry award for this performance. It had completed five million work hours without a lost time injury to either an employee or contractor. Skeptics might wonder whether this outcome was achieved by bringing the "walking wounded" back to work the day after an accident to prevent it counting as a lost time injury, a common practice in organisations which are assessed on the basis of their LTI performance. The answer to the skeptics is provided by Esso's figures on total recordable injuries, defined as injuries which require treatment by a doctor or which prevent the injured person from performing any part of their normal duties. In May 1998, just four months before the accident the company had gone six months without a single recordable injury. Finally, it should be noted that Esso's performance had been sustained; its LTI statistics for the whole period from 1990 to 1998 had been well ahead of the industry average.

To understand this paradox of how a company with such an enviable safety record was apparently so inattentive to the hazards which led to the fire we need to make a distinction between, on the one hand, high frequency low severity events such as slips, trips and falls, which result in injury to single individuals and, on the other, low frequency high severity incident**s** such as explosions and major fires, which may result in multiple fatalities. LTI data are largely a measure of the number of routine industrial injuries; explosions and major fires, precisely because they are rare, do not contribute to the LTI figures in the normal course of events. LTI data are thus a measure of how well a company is managing the minor hazards which result in routine injuries; they tell us nothing about how well major hazards are being managed. Moreover, firms normally attend to what is being measured, at the expense of what is not. Thus a focus on LTIs can lead companies to become complacent about their management of major hazards. This is exactly what seems to have happened at Esso.

Esso had achieved its remarkable record by introducing a series of initiatives explicitly aimed at preventing minor injuries. For instance, it set great store by its "step back 5 x5" program. This required workers, every time they began a new job, to take five steps back

(metaphorically) and spend five minutes thinking about the possible hazards of the job and means to control them.

Let us consider in more detail why Esso did not respond to the warnings. The petroleum coming ashore from the Bass Strait platforms is quite variable in makeup and the job of the Longford plant is to refine this product to specifications provided by Esso's customers. This variability in what enters the plant, as well as what goes out, can at times lead to "process upsets" which operators must manage. The failure to manage these upsets satisfactorily can sometimes affect the quality of product delivered to customers; it can also potentially affect the safety of the plant. The various cold temperature incidents which resulted in icing on pipes were examples of such process upsets.

Esso had a well developed incident and near miss reporting system. The reports were read daily by senior managers and there was a clear protocol about follow-up action. In practice, process upsets were not treated as incidents or near misses and were thus not reported, although they could and should have been. Even process upsets serious enough to lead to temporary shut down of the plant failed to enter the reporting system. There was no good reason for this. Management's view was that it was up to the operators to report matters if they thought they had an "escalation potential" (T4132). But in practice neither operators nor more senior staff seemed to have considered the escalation potential of process upsets. None of the warning signs referred to above was reported in either of these systems. Had they been they would have triggered investigations which would very probably have uncovered the problem which led to the disaster (T6546).

Instead, Esso's reporting systems were primarily used to report injuries to individuals, or incidents with the potential to cause injury to an individual. In this way, Esso's reporting system was transformed into a tool for dealing with lost time injuries and their value for disaster prevention was systematically undermined. According to counsel assisting the inquiry, this "lack of focus on process issues is a matter of grave concern" (T6535) . To put it bluntly Esso's focus on lost time injury rates distorted its safety effort and distracted the company's attention from the management of major hazards.

Clearly the lost time injury rate is the wrong measure of safety in any industry which faces major hazards. An airline, for instance, would not make the mistake of measuring air safety by looking at the number of routine injuries occurring to its staff. The number of injuries experienced by baggage handlers tells us nothing about flight safety. Moreover the incident and near miss reporting systems operated in the industry are concerned with incidents which have the potential for disaster, not lost time injury. Similarly, nuclear power stations in the United States have developed a number of indicators of plant safety which have nothing to do with LTIs. The challenge then is to devise ways of measuring safety in industries which face major hazards, ways which are quite independent of lost time injuries.

<u>Designing a Reporting System to Avert Disaster</u>

Prior to any disaster there will nearly always be warning signs - information somewhere within the organisation that trouble is brewing. The challenge is to find ways to assemble this

information and move up the hierarchy to the point where it can be understood and responsibly acted on.

Any company which faces major hazards is likely to have an e-mail system or something similar which can greatly facilitate the flow of information up the hierarchy. The suggestions which follow depend in large part on this kind of technology.

The starting point is an incident or near miss reporting system. But if this is to have any chance of gathering relevant warning signs, management must put considerable thought into specifying what sorts of things should be reported: what are the warning signs that something might be about to go disastrously wrong? Here are some examples:

certain kinds of leaks
certain kinds of alarms
particular temperature, pressure or other readings
maintenance not being done
dangerous work practices
machinery in a dangerous condition

Management should also consider whether anyone on site is required to fill out an end of shift report. If so, might these reports contain warning information which should be entered into the reporting system?

Workers on site should be encouraged to report not only these matters but any others about which they are concerned. In some circumstances workers will be frightened to make reports for fear of reprisals. Management will need to find ways to overcome these fears.

It is not enough that people make reports or pass information up the line. The outcome must be fed back in the form of a written response to the person who made the initial report. This will improve the morale of reporters and they will be motivated to take the reporting process more seriously. In the absence of such feedback, reporting systems are likely to break down.

To be truly effective the process must not terminate at this point. The next step is to require the person who initially raised the matter to indicate whether the action taken is satisfactory in his or her view. Where the initiator is not satisfied the matter should cycle through the system again until such time as the initiator is satisfied, or alternatively, some senior manager of the company is prepared to over-ride the concerns of the initiator, in writing.

Reporting systems must also specify a time by which management must respond, and people making reports should be able to some extent to specify how urgent the matter is and therefore how quickly they require a response, eg within a day, within a week, within a month.

Moreover, if the person to whom the report is made does not respond within the required time the system must escalate, that is, send the message further up the corporate hierarchy. This not only draws the attention of more senior managers to the problem but also alerts them to the fact that their subordinates may not be responding appropriately. This chain of escalation should end up on the screen of the CEO.

If properly implemented such systems will go a long way towards ensuring that warning of impending disaster gets to the top of the management hierarchy, into the hands of people who can do something about it. And the good news is that such systems are already commercially available.

All this depends, however, on whether the system is properly implemented. Ultimately this turns on whether the person at the top of the information chain, the CEO, is committed to making it work or not. If the CEO allows messages to sit unanswered on his or her screen the system may end up a flop. But if the CEO responds by asking why the message has not been answered further down the line, the chances are the system will work.

Such systems must also be carefully audited, that is, tested to see if they are working. One such test is to track some of the information flows which have occurred to see whether bad news, or at least news of problems, is indeed being entered into the system and responded to. Another test strategy might be to enter a significant warning into the reporting system and see how the system responds. Experience shows that no reliance should be placed on the system described above unless and until it passes these kinds of tests.

The Failure of the Alarm System

Operators at the Longford plant were required to keep operations within certain parameters (temperature, volume etc). When the process went outside these parameters alarms would both sound and light up on control panels. The sound could be, and was, silenced immediately, but the visual indicators would remain until the process returned within the specified parameters. In practice, alarms were very frequent - hundreds and sometimes thousands every day. It was clearly impossible for operators to monitor these alarms, let alone respond to them, and they had become accustomed to operating the system in alarm for long periods. Operating in alarm mode was tolerable in some circumstances, but operators had no way of distinguishing critical alarms from nuisance alarms. The result was that operators became desensitised and alarms consequently lost their capacity to serve as warnings. It was the failure to respond adequately to these alarms which led to the failure of the lean oil system which in turn led to the cold temperature embrittlement of the heat exchanger.

Other disasters have been preceded by a similar process of normalising the warning signs. Prior to the Challenger space shuttle disaster there was evidence that the so-called O-ring seals on the booster rockets malfunctioned at low temperature. But previous launches at low temperature had not ended in disaster and so the malfunction had come to be accepted as normal. On the launch date in question the atmospheric temperature was even colder than usual, but the expected malfunction had been normalised and the launch was given the go-ahead. On this occasion the O-rings failed totally with catastrophic results.

Similarly, prior to the Moura mine disaster in central Queensland in 1994 in which 11 men were killed, warning alarms had become so frequent that they were regarded as normal and so discounted (Hopkins, 1999).

Inadequate oversight by senior staff

The Royal Commission was critical of inadequate oversight of the production process by senior Esso staff. Esso had relocated all its engineers from the Longford site to head office in Melbourne in 1992. Some of these engineers were intended to operate from a distance as a "plant surveillance group" but the group did not carry out this function satisfactorily. For instance, it failed to notice or react to the frequency of alarms being generated by process upsets and it failed to recognise the danger of allowing operators to become accustomed to operating the plant in alarm mode. It was this failure of oversight which allowed critical alarms to be ignored. As the Commission put it, "the absence of regular monitoring of process operations by senior personnel in a high pressure hydrocarbon processing plant, which was not equipped with protective devices to make it completely fail-safe, exposed the plant to an unacceptable risk".

To generalise to other industries, it is vital that processes which can result in disaster be carefully managed by senior staff. Esso's policy at Longford was to leave the management of process upsets to the operators on the assumption that they knew best. In the words of the company's managing director, "operations personnel are best placed, given their experience in operating plants, to deal with operating matters including process upsets" (T5460). In the matter of disaster prevention, this is an unacceptable position.

The need for a safety case regime

Th so-called safety case approach is recognised as best practice regulation for major hazards facilities such as Longford. Safety case regimes operate in Europe and also in Australia, for the off shore oil industry. The National Occupational Health and Safety Commission has recommended it be adopted for all major hazards facilities in this country (NOHSC, 1996).

A safety case is a case which the operator of a hazardous facility makes to the regulator, setting out how safety is to be managed. It must include details of the hazard identification process, the hazards which have been identified and the procedures which have been set in place to control them. Such cases must be approved by the regulator before the facility is allowed to operate. The system remains self-regulatory in principle but rather than the facility being left to its own devices by the regulator it must convince the regulator that its strategy for managing safety is satisfactory. Under any safety case regime, facility operators are expected to adopt best practice risk management. In the oil industry this means the performance of HAZOPs on all plant.

At the time of the Longford explosion, Esso's off-shore platforms were subject to a safety case regime, administered in part by the federal Department of Primary Industry and Energy, but the Longford facility was subject only to the normal provisions of the Victorian *Occupational Health and Safety Act 1985*. Esso had performed the necessary HAZOPs off-shore but had not done so at its oldest on-shore gas plant at Longford. In a sense therefore the self-regulatory regime in Victoria had allowed Esso to fall short of best practice in the management of safety at its Longford facility. The Royal Commission concluded that all

major hazard facilities in Victoria should be required to make a safety case to an appropriate regulatory body.

Conclusion

This paper has analysed the findings of the Royal Commission into the major accident at Esso's gas plant at Longford in Victoria in 1998. In the process it has identified a number of lessons which are applicable to hazardous industries generally. It is appropriate to summarise those lessons by way of conclusion.

1 Operator error is not an adequate explanation for major accidents.
2 Systematic hazard identification is vital for accident prevention.
3 Auditing must be good enough to identify the bad news and ensure it gets to the top.
4 Reliance on lost time injury data in major hazard industries is itself a major hazard.
5 Good reporting systems must specify relevant warning signs. They must provide feedback to reporters and an opportunity for reporters to comment on feedback.
6 Alarm systems must be carefully designed so that warnings of trouble do not get dismissed as normal (normalised).
7 Senior management must accept responsibility for the management of hazardous processes.
8 A safety case regime should apply to all major hazard facilities.

REFERENCES

Appleton, B. (1994). Piper Alpha. In T. Kletz (Ed.), Lessons from Disaster: How Organisations Have No Memory and Accidents Recur . (pp. 174-184). London: Institute of Chemical Engineers.

Bahr, N. (1997), System Safety Engineering and Risk Assessment: a Practical Approach London: Taylor and Francis

Dawson, D &B Brooks, (1999) The Esso Longford Gas Plant Accident: Report of the Longford Royal Commission. Melbourne: Parliament of Victoria

Hopkins, A. (1999) Managing Major Hazards: the Lessons of the Moura Mine Disaster, Sydney: Allen & Unwin

Hopkins, A. (2000) Lessons from Longford: The Esso Gas Plant Explosion. Sydney: CCH Australia, phone1300 300 224

NOHSC -National OHS Commission - (1996) Control of Major Hazard Facilities: National Standard. Canberra: AGPS

Reason, J. (1997), Managing the Risks of Organisational Accidents. Alderlshot: Ashgate

Txxxx. This refers to the transcript page number which were obtained from http://www.vgrs.vic.gov.au/client?file.wcn. There is no hard copy of the transcript available publicly; interested readers should contact the author who has a downloaded version.