To Mary Kay O'Connor Process Safety Center Home Page
To Program details for Day 1
To Program details for Day 2

Making Safety Second Nature

Trevor A Kletz
Process Safety Consultant

Paper presented at the 1st Annual Symposium of the Mary Kay O'Connor Process Safety Center,
"Beyond Regulatory Compliance, Making Safety Second Nature",
George Bush Presidential Conference Center, College Station, Texas
March 30-31, 1998.

MAKING SAFETY SECOND NATURE

Trevor A Kletz

Abstract

From the 1960s onwards the chemical and oil industries developed and used a number of new safety techniques which, in time, became second nature to those who used them. They included the use of QRA for deciding priorities, Hazop and audits for identifying problems, inherently safer design for avoiding hazards, and more thorough investigation of incidents for identifying underlying causes. However, it has not yet become second nature to remember the accidents of the past and the actions needed to prevent them happening again.

I joined industry in 1944 and moved to production in 1952. Then, and for at least 15 years afterwards, safety was a non-technical subject that could be left to arts graduates and elderly foremen. There was concern that people should not be hurt - great attention was paid to the lost-time accident rate - but there was no realization that it was a subject worthy of systematic study by experienced technologists.

This view changed at the end of the 1960s. A new generation of plants had been built, operating at higher temperatures and pressures and containing larger inventories of hazardous chemicals; the result was a series of fires and explosions and a worsening fatal accident rate. Figure 1 shows the situation in ICI, at the time the UK's largest chemical company. Other companies were similar.

As a result in 1968, I was appointed one of the company's first technical safety advisers, an unusual appointment at the time for someone with my experience, and if the reason for my appointment had not been so obvious I would have wondered what I had done wrong. I and my colleagues tried to apply to safety the same sort of systematic thinking that we applied in our other professional work. We developed some new ideas and techniques and adopted others. A common feature of them, realised only in retrospect, was that they were more than mere problem-solving techniques. Once people had got used to these new concepts and used them a few times they began to look at a whole range of problems in a different way.

Quantitative risk assessment (QRA)

I realised as soon as I was appointed that we could not do everything at once. Some problems had to be left alone, at least for the time being. We needed a rational and defensible method of deciding priorities. The method we used, whenever practicable, was to compare the risk to life from the various hazards to which employees were exposed. To do this we had to set a target or criterion: risks above the target were to be reduced as matter of priority; those below could to be left alone, at least for the time being. We called the technique hazard analysis or Hazan but today it is better known as risk assessment or QRA [1, 2].

Our openness about risks which we intended to ignore, at least for the present, surprised some of my American friends. Our approach was accepted in the UK because our law has long recognized that we cannot do everything possible to prevent accidents. We are required to do only what is reasonably practicable, weighing in the balance the cost of prevention, in money, time and trouble, and comparing it with the size of the risk. If there is a gross disproportion between them, the risk being insignificant in relation to the cost, removal of the risk is considered to be not "reasonably practicable". I hope I am not being unfair to OSHA when I say that their attitude at the time seemed to be, "If an accident is possible, prevent it. Don't tell me it is unlikely to occur, small in its effects and expensive to remove; just remove it".

However, the point I want to emphasis today is that once people have carried out a number of risk assessments they start to look at problems differently. Instead of saying, "There is a hazard, how can I control it?", they are more likely to say, "How likely is it to happen? How serious will the consequences be? Should we spend resources on it or would the money be better spent on the removal or control of other hazards?"

At first we applied QRA to in-plant problems - those that could only affect the workforce - and it was easy to set a target: do rather better that in the past. When we extended the technique to risks that could affect the public, setting a target was much more difficult as no member of the public has been killed in the UK this century by an accident in a chemical plant. The past, in this respect, was perfect. We therefore based our target on a comparison with other risks that the public accept without complaint. The first example of this was a paper by Siccama [3], from the Netherlands, who suggested that his fellow countrymen should accept the same risk from the storage of hazardous chemicals that they already openly accepted from flooding of the dikes. However, the public's tolerance of risks is based on their perceptions of them rather than their actual size and on whether they are natural or man-made. Technologists have been slow to realise this and it has not yet become second nature. Many of us are still irritated by the public's reluctance to recognise the safety and value of the chemical industry [4].

Hazard Identification

Once we started to use QRA we soon realised that the biggest source of error was not in the QRA itself but in a failure to foresee all the hazards or all the ways in which they can occur. We were estimating the probability and consequences of the hazards we recognized with ever greater accuracy while possibly ignoring greater hazards. We realized that it was little use carrying out a QRA until we had systematically tried to identify the hazards by a hazard and operability study or Hazop, a technique developed in ICI in 1963 [2].

Those who have taken part in Hazops are never quite the same again. They learn to look more critically at designs and proposals and to see some of the things that might go wrong. No individual alone can carry out a Hazop, the technique depends on interactions between the members of the team, but those who have experience of them have an increased awareness of possible pitfalls in design.

Carling has described the results of using Hazop in his company [5]. The benefits went far beyond a simple list of recommendations for a safer plant. The interaction between team members brought about a profound change in individual and departmental attitudes. Staff began to seek one another out to discuss possible consequences of proposed changes, problems were discussed more openly, departmental rivalries and barriers receded. The dangers of working in isolation and the consequences of ill-judged and hasty actions became better appreciated. Knowledge, ideas and experience became shared more fully to the benefit of the individual and the company. I have described elsewhere how the need for complex (and unsuccessful) protection could have been avoided by moving some equipment a few meters from a Division 2 to a safe area, if the various design sections had discussed it together instead of passing the design on from one section to another [7].

The explosion at Flixborough in 1974, when 28 people were killed and the plant destroyed, drew attention to the unforeseen results of plant modifications, often quite simple ones, and many companies have introduced control procedures [6]. However, accidents still occur, all too often, because the procedures are not always followed. People are still inclined to say, "It's only a minor change, just an extra valve, what could possibly go wrong?" Too late, they discover that it isolated a vessel from its relief valve or leaked and contaminated a product."

Inherently safer design

From 1968 to 1974 my colleagues and I concentrated on the technical hazards and left 'hard hat' safety to others. However, we all shared the view that plants were made safer by adding on protective equipment or procedures, from hard hats to complex interlocks. This changed after the explosion at Flixborough. The leak and explosion were so large and the results so serious because the unit, a stage in the manufacture of nylon, contained a large inventory of flammable hydrocarbon. It contained so much because only about 6 percent of the feedstock was reacted per pass, the rest getting a free ride, in fact, many free rides, and having to be recovered and recycled. If the inventory could be reduced then the hazard would be removed or reduced. The plant would be safer, not because we had added on protective equipment which might fail or be neglected but because we had removed or reduced the hazard; the plant would be inherently safer [7,8].

Reducing the inventory in the Flixborough process is not easy and the only company that tried to do so soon abandoned the work as they could foresee no need for a new plant. However, there were many other examples of the successful introduction of inherently safer designs, notably the latest process for the manufacture of nitroglycerine. We set out to advocate these designs and in 1984 Bhopal drew attention again to the desirability of doing so. The material that leaked and killed over 2000 people was not a product or raw material but an intermediate. It was convenient to store it but not essential to do so, a point missed by most commentators [9].

No change with which I have been associated is more fundamental that this one. Whenever possible we should avoid or remove hazards rather than keep them under control. We should keep lambs rather than lions. There has been real progress but it has been nothing like as rapid as in the case of QRA or Hazop. The changes necessary - the realization that inherently safer designs are possible and a deliberate systematic search for them in the early stages of design - are so fundamental that they cannot occur quickly. They need the active involvement of senior people, most of whom are still unfamiliar with the concept. Those who have grasped the concept and put it into practice never look at plant designs in the same way again. For them protective equipment and procedures and analysis of them by QRA is a second best, to be followed only when an inherently safer design is impracticable. Before we spend time estimating the size of a hazard we should ask if it could be removed.

Audits

Most companies now carry out safety audits. Some of the most effective audits, however, are those carried out by supervisors and superintendents on their normal plant tours. Once they have trained themselves to keep their eyes open they will find that they see a lot more. As a manager, not a safety adviser, I took a camera on plant tours and showed the resulting slides at staff meetings. People were horrified to see the hazards they had passed every day without noticing them.

Accident investigation and human error

Even before my full-time involvement in safety I had become aware that many accident investigation reports were superficial, dealing only with the immediate technical causes and paying no attention to ways of avoiding the hazard or weaknesses in the management system [10, 11]. Thus to say a leak is due to corrosion is superficial. We need to ask if corrosion could have been foreseen and a different material of construction used, if the specified material was actually used, if operating conditions were in the range given to the designer, if regular tests and inspections were needed, if they were actually carried out and, if so, what was done with the results. The answers to these questions will raise fresh ones!

Superficiality is most pronounced when human error is quoted as the cause of an accident, as it so often is. In a sense every accident is due to human error, by operator, designer or manager. However, when a report says that an accident was due to human error the writer usually means an error by an operator or someone else at the bottom of the pile who cannot blame someone below him. Managers and designers, it seems are not human or do not make errors.

A more serious weakness in calling human error a cause is that errors are made for different reasons and quite different actions are needed to prevent them happening again. Some errors occur because someone does not know what to do, some because they know what to do but decide not to do it, some because the action needed is beyond the physical or mental ability of the person expected to do it, perhaps beyond anyone's ability, and some are due to a slip or lapse of attention. Those in the last group are the most common and are very difficult to prevent. Telling people to be more careful is simply dodging the issue. The only satisfactory solution is to remove opportunities for error by changes in design or methods of working. This is related to the inherently safer designs discussed above. If a flammable solvent has been replaced by a non-flammable one errors of whatever type cannot cause a solvent fire.

If senior managers accept superficial accident reports then people will continue to produce them. If senior managers insist that underlying causes are uncovered, doing so will soon become second nature and accidents will be turned into learning experiences.

Remembering the lessons of the past

Whether accident reports are thorough or superficial in most companies they are soon forgotten, the new procedure introduced after the last accident are allowed to lapse and the accident happens again. Here are some actions we can take to keep alive the memories of the past, actions which, in most companies, have still to become second nature [12]:

> Include in every instruction, code and standard a note on the reasons for it and accounts of accidents which would not have occurred if the instruction, code or standard had been followed.
>
> Describe old accidents as well as recent ones in safety bulletins and newsletters and discuss them at safety meetings. "Giving the message once is not enough".
>
> Follow up at regular intervals to see that the recommendations made after accidents are being followed, in design as well as operations.
>
> Remember that the first step down the road to the next accident in this series occurs when someone turns a blind eye to a missing blind.
>
> Never remove equipment before you know why it was installed. Never abandon a procedure

before you know why it was adopted.

Devise better retrieval systems so that we can find, more easily than at present, details of past accidents, in our own and other companies, and the recommendations made afterwards. Few companies make full use of the computerized information systems that are available and even where there is a system, few employees seem to use it. If such a system is to be widely used it must available at everyone's desk. It will not be widely used if we have to walk to the library and/or consult an information scientist. We need (and it is being developed) is a system that will use the information already entered for other purposes to remind the operator, the designer and the person preparing a permit-to-work of hazards that they may not be aware of, or have overlooked. The computer will be active and the human will be passive [13].

Include important accidents of the past in the training of undergraduates and company employees. Compared with the large number of courses on hazard identification and assessment, few courses cover these subjects. Suitable training material is available, for example, from the UK Institution of Chemical Engineers, but local accidents have more impact.

The last suggestion is probably the most valuable. I spent a lot of time on discussions of past accidents when I was a safety adviser. Discussions are better than lectures as more is remembered, especially if those present are encouraged to say what they think should be done. Most of the technical staff attended such a discussion every year and over time it produced a significant change in attitude. But note, I did not set out to change attitudes; I set out to give my colleagues the knowledge and understanding they needed to prevent accidents and I did so by getting them to work it our for themselves.

If safety isn’t second nature

What can we do if our colleagues do not use these techniques I have discussed? We can:

Suggest that they try them and see if they find them helpful?

Publicize case histories, preferably local, of the successful application of hazop, QRA, inherently safer design etc.

Get your senior managers to encourage their use.

Compliance

When I started as safety adviser, and before that as line manager, compliance with the law was a minor part of my activities. My colleagues and I did what we considered necessary for the protection of our employees, the public and the company's investment and as result did far more that the law required. Since then the number of laws to be obeyed has increased, everywhere, and there is a tendency for people to say, "It must be safe as I am following all the rules". This is not true. This attitude must not be allowed to become second nature. I feel there is something wrong when the safety advisers in a company are part of a Regulatory Affairs Department headed by a lawyer.

Final thoughts

There is a welcome interest today in safety management systems but we must not forget their limitations. All that a system can do is harness the knowledge and experience of people. If knowledge and experience have been downsized away the system is an empty shell. Knowledge and experience without a system will achieve less than their full potential. Without knowledge and experience a system will achieve nothing.

In every walk of life, if comments are based, as mine are, on past experience, someone will say, "Schools/hospitals/offices/factories aren't like that any more." Is old information still relevant? In many ways factories, at least, ARE like they used to be as human nature is a common factor. We may have better equipment but may be just as likely as in the past to cut corners when we design, construct, operate, test and maintain it, perhaps more likely as there are fewer of us to keep our eyes open as we go round the plant and follow up unusual observations. We may have access to more knowledge than our parents and grandparents, but are we any more thorough and reliable?

I have worked in industry as a line manager with the authority, in theory, to impose my views and as an adviser who can only persuade. If one can give people the skill and knowledge to decide for themselves what is safe (empower them in today's management jargon), then their convictions will survive after one has left, they will have become second nature. In contrast, practices imposed by authority lapse when the boss moves on or, more often, when he or she loses interest.

The loss of the Piper Alpha oil platform in the North Sea was the result of management failure, a failure to enforce a permit-to-work system [10,14]. The top men in Occidental were not hard-nosed and uncaring people interested only in profit and unconcerned about safety. They said and believed all the right things; they said that safety was important but they did not get involved in the precise actions required, see that they were carried out and monitor progress.

Safety is not an intellectual exercise to keep us in work. It is a matter of life and death. It is the sum of our contributions to safety management that determines whether the people we work with live or die. On Piper Alpha they died. - *Brian Appleton, Technical assessor to the public inquiry*

References

Kletz, T. A., 1971, Hazard Analyse - A quantitative approach to safety, *Symposium Series No 34*, Institution of Chemical Engineers, Rugby, UK, p. 75.

Kletz, T. A., 1992, *Hazop and Hazan - Identifying and Assessing Process Industry Hazards,* 3rd edition, Institution of Chemical Engineers, Rugby, UK, 1992.

Siccama, E. H., 1973, *De Ingenieur*, 85(24):502.

Kletz, T. A., 1996, *Disaster Prevention & Management*, 5(4):41.

Carling, N., 1987, Hazop study of BAPCO's FCCU complex, API Committee on Safety and Fire Protection Spring Meeting, Denver, CO, 8-11 April.

Sanders, R. E., 1983, *Management of Change in Chemical Plants - Learning from Case Histories*, Butterworth-Heinemann, Oxford, UK.

Kletz, T. A, 1998, *Plant Design for Safety - A User-Friendly Approach*, 2nd edition, Taylor & Francis, Washington, DC.

Crowl, D. A. (ed.), 1996, *Inherently Safer Chemical Processes*, AIChE, New York.

Kletz, T. A., 1994, *Learning from Accidents*, 2nd edition, Butterworth-Heinemann, Oxford, UK, Chapter 10.

Kletz, T. A., 1994, *Learning from Accidents*, 2nd edition, Butterworth-Heinemann, Oxford, UK.

Kletz, T. A., 1991, *An Engineer's View of Human Error*, 2nd edition, Institution of Chemical Engineers, Rugby, UK.

Kletz, T. A., 1993, *Lessons from Disaster - How Organisations have No Memory and Accidents Recur*, Gulf, Houston, TX and Institution of Chemical Engineers, Rugby, UK.

Chung, P. W. H., Integration of accident database with computer tools, Institution of Chemical Engineers Research Event, Newcastle, UK, 7-8 April 1998.

14.Cullen, Lord, 1990, *The Public Inquiry into the Piper Alpha Disaster*, Her Majesty's Stationery Office, London.

To Mary Kay O'Connor Process Safety Center Home Page
To Program details for Day 1
To Program details for Day 2