IMPROVING SAFETY PERFORMANCE IN THE NEW MILLENNIUM AND THE ROLE OF UNIVERSITIES

Trevor Kletz

Department of Chemical Engineering, Loughborough University, UK

Abstract

Although the safety record of the process industries is good, almost all the accidents that occur need not have occurred. Often, after an accident or near-miss, we neglect opportunities to learn and remember:

- Accident reports identify only a single cause.
- They are often superficial, dealing only with the immediate causes. We should also look for ways of avoiding the hazards, such as inherently safer design, and for weaknesses in the management system.
- They often list human error as a cause without saying what sort of error. Yet different actions are needed to prevent those due to ignorance, those due to slips or lapses of attention and those due to non-compliance.
- They often list causes we can do little about.
- We do not allow others to learn as much as they could from our experiences.
- We forget the lessons learned and the accident happens again. We need better training, by describing accidents first rather than principles, as accidents grab our attention, and we need discussion rather that lecturing, so that more is remembered. We need databases that can present relevant information without the user having to ask for it.

Some actions that universities might take are discussed.

- - - - - - - - -

The chemical industry is a much safer place to work than many industries with fewer inherent hazards[1]. Nevertheless, almost all the accidents that have occurred need not have occurred. Most of them have happened before and have been described in published reports. Someone knew how to prevent them even if the people on the job at the time did not. There is something seriously wrong with our safety training and the availability of information if preventable accidents keep on happening.

Having paid the price of an accident, minor or serious (or narrowly missed), we often neglect the opportunity to learn from it. Failures should be seen as educational experiences for both the individual and the organization. Six major opportunities are frequently missed, the first four during the preparation of the report and the other two afterwards.

1 Accident reports are often one-dimensional, that is, they identify only a single cause. Their authors do not realize that that many people, from the chemist who chose the process, through the designers, down to the last link in the chain, the operator who closed the wrong valve, have an opportunity to prevent every chemical accident. Often the single cause identified is the last link in the chain, the person who closed the wrong valve or the mechanic who broke the wrong joint.

Just as we are blind to all but one the octaves in the electromagnetic spectrum so we are blind to many of the ways of preventing an accident.

2 Even when we look for and find more than one cause **the reports are often superficial,** dealing only with the immediate causes. We should look beyond them for ways of avoiding the hazards, such as inherently safer design, and for weaknesses in the management system. Today many, but by no means all, companies pay more attention to the other links in the chain of events that led to the accident. For example, could less hazardous raw materials have been used? Could more safety features have been included in the design? Were the operators adequately trained and instructed? If a mechanic opened up the wrong piece of equipment, why wasn't there a better system for identifying it? Saying, "The pump you repaired last week is giving trouble again" is a recipe for an accident. Were previous incidents overlooked because the results were, by good fortune, only trivial? The emphasis has shifted from blaming the operator to removing opportunities for error or identifying weaknesses in the design and management system.

For example, most commentators on Bhopal missed the most important lesson that can be drawn from it: 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 and afterwards many companies did reduce their stocks of hazardous intermediates, often using them as they were made and replacing 50 or more tons in a tank by a few kilograms in a pipeline. For ten years since the explosion at Flixborough in 1974, the importance of keeping stocks of hazardous chemicals as low as possible had been advocated but little had been done. Minimum stocks are not only safer, but also cheaper. In this example more safety does not mean more cost. If we can avoid hazards we can often design plants that are cheaper as well as safer.

The report on a serious explosion which killed four men shows how easily underlying causes can be missed. The explosion occurred in a building where ethylene gas was processed at high pressure. A leak from a badly made joint was ignited by an unknown cause.

After the explosion many changes were made to improve the standard of joint-making: better training, tools and inspection.

Poor joint-making and frequent leaks had been tolerated for a long time as all sources of ignition had been eliminated and so leaks could not ignite, or so it was believed. The plant was part of a large group but the individual parts of it were technically independent. The other plants in the group had never believed that leaks of flammable gas will not ignite. Experience had taught them that sources of ignition are liable to turn up, even though we do everything we can to remove known sources, and therefore strenuous efforts must be made to prevent leaks and good ventilation provided to disperse any that do occur. Unfortunately the managers of the plant involved in the explosion had hardly any technical contact with the other plants, though their sites adjoined. Handling flammable gases at high pressure was, they believed, a specialized technology and little could be learnt from those who handled them at low pressure. The factory was a monastery, a group of people isolating themselves from the outside world. The explosion blew down the monastery walls.

If the management of the plant where the explosion occurred had been less insular and more willing to compare experiences with other people in the group, or if the directors of the group had allowed the component parts less autonomy, the explosion might never have occurred. The senior managers of the plant or the group probably never realized or discussed the need for a change in policy. The leak was due to a badly made joint and so joints must be made correctly in future. No expense was spared to achieve this aim but the underlying weaknesses in the company organization and plant design were not recognized. However, some years later, during a recession, parts of the group were merged.

There is another example in the Appendix.

3 Human error is often listed as a cause but is far too vague a term to be useful. We should ask, "What sort of error?"

- Was it due to poor training or instructions? If so we need improve them and perhaps simplify the task.

- Was it due to a deliberate decision not to follow instructions or recognized good practice? If so, we need to explain the reasons for the instructions as we do not live in a society in which people will simply do what they are told. We should, if possible, simplify the task – if an incorrect method is easier than the correct one it is difficult to persuade everyone to use the correct method - and check from time to time that instructions are being followed.

- Was the task beyond the ability of the person asked to do it, perhaps beyond anyone's? If so, we need to redesign the task.

- Was it a slip or lapse of attention? If so, it no use telling people to be more a careful, we should remove opportunities for error by changing the design or method of working.

4 We often list causes we can do little about. For example, a source of ignition is often listed as the cause of a fire or explosion. But, as we have just seen, it is impossible on the industrial scale to eliminate all sources of ignition with 100% certainty. While we try to remove as many as possible it is more important to prevent the formation of flammable mixtures.

For example, which is the more dangerous action on a plant that handles flammable liquids: to bring in a box of matches or to bring in a bucket? Many people would say that it is more dangerous to bring in the matches, but nobody would knowingly strike them in the presence of a leak and in a well-run plant leaks are small and infrequent. If a bucket is allowed in, however, it may be used for collecting drips or taking samples. A flammable mixture will be present above the surface of the liquid and may be ignited by a stray source of ignition. Of the two “causes“ of the subsequent fire, the bucket is the easier to avoid.

I am not, of course, suggesting that we allowed unrestricted use of matches on our plants but I do suggest that we keep out open containers as thoroughly as we keep out matches.

Instead of listing causes we should list the actions needed to prevent a recurrence. This forces to people to ask themselves if the so-called cause can be prevented in future.

5 We do not allow others to learn from our experiences. Many companies restrict the circulation of incident reports as they do not want everyone, even everyone in the company, to know that they have blundered but this will not prevent the incident happening again. We should circulate the essential messages widely, in the company and elsewhere, so that others can learn from them, for several reasons:

- *Moral:* if we have information that might prevent another accident we have a duty to pass it on.

- *Pragmatic:* if we tell other organizations about our accidents they may tell us about theirs.

- *Economic:* we would like our competitors to spend as much as we do on safety.

- *The industry is one: every accident effects its reputation*. To misquote the well-known words of John Donne,

> *No plant is an Island, entire of itself; every plant is a piece of the Continent, a part of the main. Any plant's loss diminishes us, because we are involved in the Industry: and therefore never send to know for whom the Inquiry sitteth; it sitteth for thee.*

6 We forget the lessons learned and allow the accident to happen again. Preparing a good report is not enough. All too often the report is read, filed and forgotten. Organizations have no memory. Only people have memories and after a few years they move on taking their memories with them. Procedures lapse or the equipment falls out of use and the accident happens again, even on the plant where it happened before. Or by good fortune the results are not serious and little action is taken. Reference 2 describes many examples but here is a more recent one[3]:

During cold weather a water line froze and ruptured inside a building. Damage was fortunately not very serious. Three years later the same line froze and ruptured again. The heating in the building was not operating and the water line was near the door. The basement was flooded and two 15 m^3 (4000 US gallons) tanks floated, reached the ceiling and pushed it up by 0.5 m. The incident occurred at a nuclear site. Can we blame the public for doubting the nuclear industry's ability to operate reactors safely when they let a water line freeze and rupture twice?.

To prevent the same accidents recurring we should:

- Include in every instruction, code and standard a note on the reasons for it and accounts of accidents that would not have occurred if the instruction etc had been followed.
- Never remove equipment before we know why it was installed. Never abandon a procedure before we know why it was adopted.
- Describe old accidents as well as recent ones in safety bulletins and discuss them at safety meetings.
- 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 an accident occurs when someone turns a blind eye to a missing blind.

- Include important accidents of the past in the training of undergraduates and company employees.

- Keep a folder of old accident reports in every control room. It should be compulsory reading for new employees and other should look through it from time to time.

- 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. We need systems in which the computer will automatically draw our attention to information that is relevant to what we are typing (or reading), as described below.

6.1 Weaknesses in safety training

As already stated, there is something seriously wrong with our safety education when so many accidents repeat themselves so often. It is, I believe, too theoretical. It starts with principles, codes and standards. It tells us what we should do and why we should do it and warns us that we may have accidents if we do not follow the advice. If anyone is still reading or listening it may then go on the describe some of the accidents.

We should start by describing accidents and draw the lessons from them, for two reasons. First, accidents grab our attention and make us read on, or sit up and listen. Suppose an article describes a management system for the control of plant and process modifications. We probably glance at it and put it aside to read later, and you know what that means. If it is a talk we probably yawn and say to ourselves, “Another management system designed by the safety department that the people on the plant won’t follow once the novelty wears off”. In contrast, if someone describes accidents caused by modifications made without sufficient thought we are more likely to read on or listen and consider how we might prevent them in the plants under our control. We remember stories about accidents far better than we remember naked advice. We all remember the stories about Adam and Eve and Noah’s Ark far better than all the dos and don’ts in the Bible.

The second reason why we should start with accident reports is that the accident is the important bit: it tells us what actually happened. We may not agree with the author’s recommendations but we should not ignore the event. If the accident could happen on our plant we know we should take steps to prevent it, though not necessarily what the report suggests.

It is far better to discuss accidents than just describe them. Outline the accident and let the audience question you to find out the rest of the facts, the facts that they think are important

and that they want to know. Then let them say what they think ought to be done to prevent it happening again. More will be remembered and the audience will be more committed than if they were merely told what to do.

6.2 What sort of reports?

We should, of course, choose for discussion (or lecture) accidents which bring out important messages such as the need for permits-to-work, control of modifications, inherently safer designs and so on. In addition, we should remember the following:

If possible, discuss accidents that occurred locally. The audience cannot then say, "We wouldn't do anything as stupid as the people on that plant".

Choose simple accidents. Many engineers are fascinated by complex stories in which someone had to puzzle out some unusual causes. Most accidents are not like that but have quite simple causes. After a fire, one company gave a lot of publicity to an unusual source of ignition and successfully distracted attention from the poor design and management that allowed four tons of hot hydrocarbon to leak out of the plant. No one asked why it leaked or how they were going to prevent it leaking again.

Draw attention to the fact that many people have opportunities to prevent accidents, starting with the chemist who chooses the process, through the engineers who design the plant and ending with the operator who closed the wrong valve. Operators often fall into the traps that others have laid for them and are the people with least responsibility.

6.3 Safety databases

There are a number of databases containing accident reports and other information. It should be easier than it ever has been to find out what accidents have occurred involving the equipment, chemicals or processes that we use. But these databases not being used as much as we hoped they would be, for several reasons. Which databases should we use? Some are on-line and others on CD-Rom. They use many different search engines each of which we have to learn to use. Searching can take a long time. But most important of all, we will look up a database only when we suspect that there might be a hazard. If we don't suspect there may be a hazard we don't look.

In conventional searching the computer is passive and the user is active. The user has to ask the database if there is any information on, say, accidents involving check valves or cyclohexane. We need a system in which the user is passive and the computer is active. With such a system, if someone is using a word processor, a design program or a Hazop recording

program and types the words check valve or cyclohexane (or perhaps even makes a diary entry that there is going to be a meeting on check valves or cyclohexane) the computer will signal that the database contains information on these subjects. A click of the mouse will then display the data. As I type these words the spellcheck and grammar check programs are running in the background drawing my attention to my (frequent) spelling and grammar errors. In a similar way, a safety database could draw attention to any subject on which it has data. Obviously, filters could prevent it repeatedly referring to the same hazard.

A program of this type has been developed for medical use. Without the doctor taking any action the program reviews the information on symptoms, treatment, diagnosis etc already entered for other purposes and suggests treatments that the doctor may have overlooked or not be aware of.

When we are aware that there is or may be a hazard and carry out conventional searching it is hindered by another weakness: It is hit or miss. We either yet a "hit" or we don't. Suppose we are looking in a safety database to see if there are any reports on accidents involving the transport of sulfuric acid. Most search engines will display them or tell us there are none. "Fuzzy" search engine will offer us reports on the transport of other minerals acids or perhaps on the storage of sulfuric acid. This is done by arranging keywords in a sort of family tree. If the there are no reports on the keyword, the system will offer reports on its parents or siblings.

There is ample power in modern computers to do all that I suggest. We just need someone willing to develop the software. It will be more difficult to consolidate various databases into one and to make the program compatible with all the various word processor, design, Hazop and control programs in use.

6.4 What could universities do?

In the United Kingdom all chemical engineering students get some training in process safety, mostly by lecture but many have to apply Hazop in their design project. In the United States most chemical engineering students do not get any significant safety training, though there are some notable exceptions.

Undergraduate training should include discussion of some accidents, chosen because they illustrate important safety principles such as the need for inherently safer design, the identification and assessment of hazards, the science of fires and explosions and the need to look below the immediate technical causes for ways of avoiding the hazard and for weaknesses in the management system. Discussion, as already mentioned, is more effective than lecturing but more time-consuming.

Universities are ideally placed to carry out research on passive searching and fuzzy searching. It has the advantage that it does not need expensive experimental facilities. At Loughborough we have demonstrated the feasibility of the latter and carried out some work on the former. As with many university projects, the work stopped when the funds ran out[4,5,6,7].

Appendix: Another example to show there are many of preventing an accident

This example is imaginary but the individual steps have all contributed to other accidents. A bellows was incorrectly installed so that it was distorted. After some months it leaked and the escaping vapour was ignited by a passing vehicle. Damage was extensive as the surrounding equipment had not been fire-protected, to save cost.

The leak would not have occurred, or the damage would have been less, if:

1 Bellows were not allowed on lines carrying hazardous materials.

2 The use of bellows had been questioned during design. Was a hazard and operability study carried out?

3 The fitter who installed the bellows had done a better job. Did he know the correct way to install a bellows and did he realize the consequences of incorrect installation?

4 There had been inspection after construction and regular inspections of items of equipment whose failure could have serious consequences.

5 Gas detectors and emergency isolation valves had been installed.

6 The plant had been laid out so that vehicles delivering supplies did not have to pass close to operating equipment.

7 There had been better control of vehicle movements.

8 The fire protection had been better.

9 An expert in process safety was involved during design, as he would have drawn attention to items 3, 5, 6, 7 and 8.

There were thus at least nine opportunities for breaking the chain of events leading to the damage and many people who could have broken it. They were all responsible to some extent and it would be wrong and unfair to pick on one or two of them and make them the culprits. The following chain diagram summaries the events that preceded the accident and shows how they could have been prevented or mitigated.

Event **Recommendations for Prevention/Mitigation**

Extensive damage
|
|----------Better fire-protection
|
Fire
|
Ignition by passing vehicle
|
|----------Better control of vehicle movements
| Better layout
|
Leak
|
|----------Install gas detectors & emergency isolation valves
| Regular inspections
|
Bellows installed incorrectly
|
|----------Better training of fitters
| Better inspection after construction
|
Decision to use bellows
|
|----------Critical examination of designs by Hazop or similar technique
|
Decision to allow use of bellows
|
|----------Do not use bellows in lines carrying hazardous materials
| More involvement by process safety experts in design
|

1. Sanders, R., *Chemical Process Safety – Learning from Case Histories,* Butterworth-Heinemann, Boston, MA, 1999, Chapter 1.

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

3. *Operating Experience Summary,* No 2000-3, Office of Nuclear and Facility Safety, US Dept. of Energy, Washington, DC, 2000.

4. Chung, P. W. H. and Jefferson, M., A fuzzy approach to accessing accident databases, *Applied Intelligence*, Vol. 9, p. 129.

5. Iliffe, R. E., Chung, P. W. H., and Kletz, T. A., More Effective Permit-to-Work Systems, *Process Safety and Environmental Protection*, Vol. 77B, March 1999, p. 69.

6. Iliffe, R. E., Chung, P. W. H., and Kletz, T. A., Hierarchical Indexing, Some lessons from Indexing Incident Databases, *International Seminar on Accident Databases as a Management Tool*, Antwerp, Belgium, November 1998.

7. The Application of Active Databases to the Problems of Human Error in Industry, Iliffe, R. E., Chung, P. W. H., Kletz, T. A., and Preston, M., *Journal of Loss Prevention in the Process Industries*, Vol.13, No.1, 2000, p. 19.