Stories to keep us safe – Five decades of the Loss Prevention Bulletin

Fiona Macleod, Managing Director, Billions Europe Ltd., Winder House, Kingfisher Way, Stockton-on-Tees, TS18 3EX

In his book, *Lessons from Disaster*, Trevor Kletz, a gifted storyteller, explains why preventable accidents recur and gives some suggestions for improving corporate memory: among them a "memory book" - a collection of investigation reports into process safety accidents and incidents.

The Loss Prevention Bulletin (LPB) could be considered the process safety memory book of the IChemE with descriptions of process and allied industry incidents drawing out the lessons learned and sharing best practice to prevent repetition.

This paper will use examples drawn from five decades of the LPB, to illustrate each of the conference themes:

1. ASSURANCE - Cyber threats to process safety
2. ENGINEERING AND DESIGN - Inherent Safety
3. ENVIRONMENTAL PROTECTION - Natural hazards
4. HUMAN FACTORS - Alarm rationalisation
5. KNOWLEDGE AND COMPETENCE - Case histories
6. SAFETY CULTURE - Corporate memory
7. SYSTEMS AND PROCEDURES -Management of Change

And will discuss

- What have we learned and what has changed in five decades?
- What has not and will never change?
- How should we respond?

Introduction

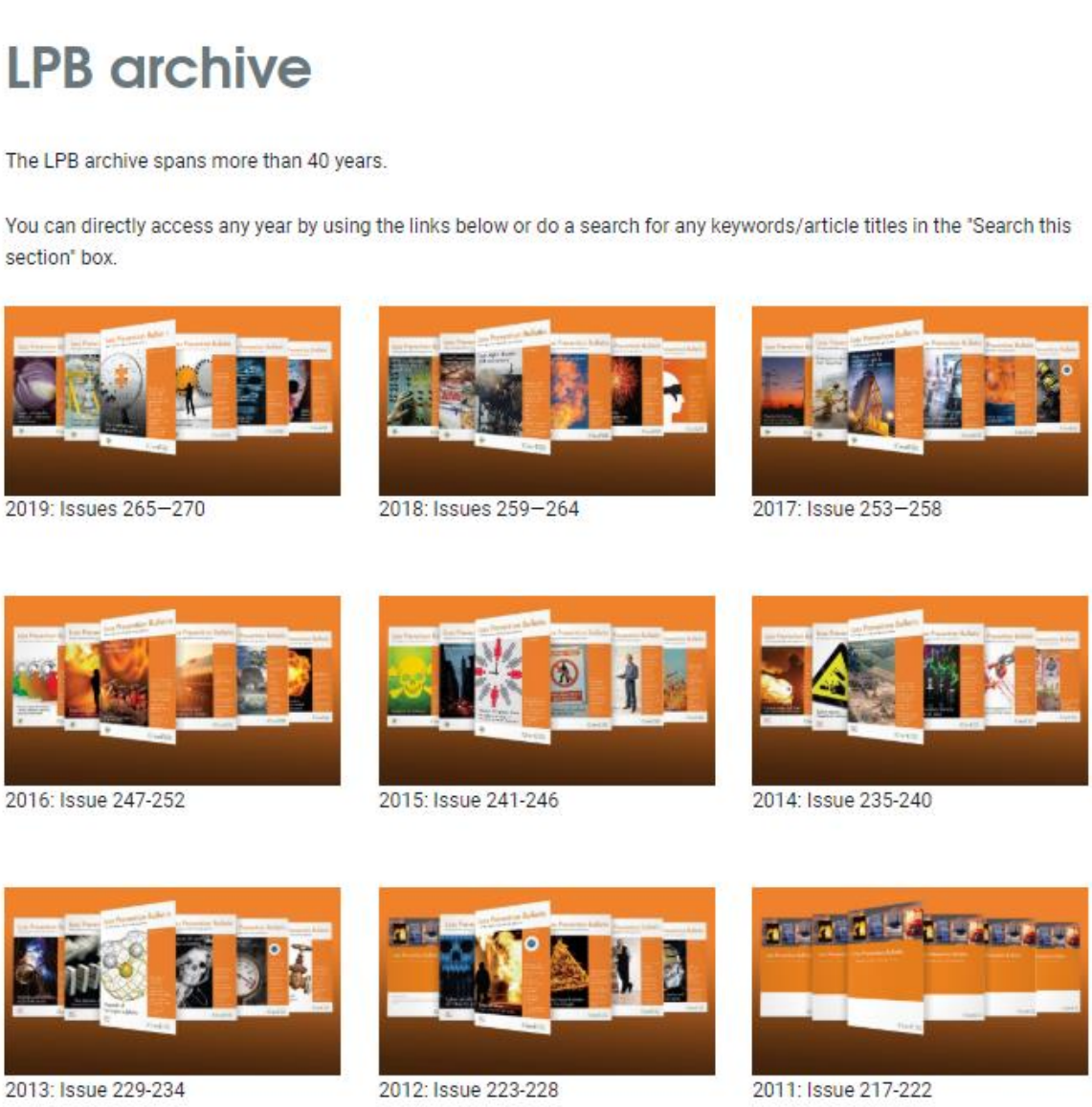
Trevor Kletz claimed that there are no new accidents[1]. The same things have happened before, for similar reasons, but those involved in the latest accident were unaware of the previous lessons learned. He also claimed that organisations have no memory. When the people who work for an organisation move on, valuable experience leaves with them.

One way to avoid new accidents is to understand old ones. The Loss Prevention Bulletin (LPB) was started by Trevor Kletz, Ted Kantyka and other like-minded process safety practitioners to record stories of accidents in order to prevent the same things happening again.

LPB Archive

The Loss Prevention Bulletin now has almost 300 papers – stories, case studies & best practice - what to do, and what not to do. In 2019, the LPB archive moved to a new platform which is easier to access and search.

[1] Kletz T A, Lessons from disaster-How organisations have no memory and accidents recur, Institution of Chemical Engineers, 1993



Screenshot from LPB website accessed 16 Jan 2020

Using the improved search facilities, we can look at each of the conference topics.

In this paper, I am going to share a few stories, in the hope that even if you don't remember the details, you will remember that there is a rich resource available in the LPB.

And perhaps you will go and take a look for yourself.

1. ASSURANCE – Cyber Security

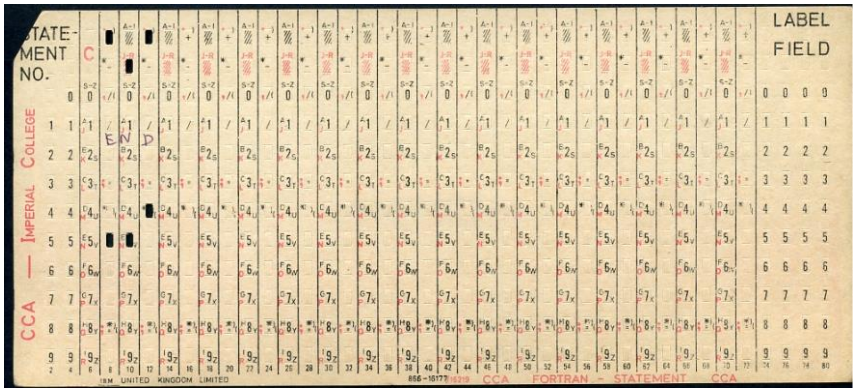
One theme of the conference is Assurance.

Safety assurance is the means to demonstrate that organisational arrangements and processes … are properly applied and continue to achieve their intended objectives. ***Safety Assurance should be intrusive and enquiring and not simply an administrative "box ticking" exercise[2].***

A new area for process safety assurance is Cyber Security.

Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, software and data from attack, damage or unauthorised access. For the process industries, this means understanding how our process control and safety systems are kept separate from business enterprise systems, which are often connected to the internet.

Cyber attack - malicious attempts to interfere with computer systems - was not something that troubled early process safety professionals. I remember my first encounter with a computer in 1980. I dropped a stack of 186 unnumbered punch cards while rushing between the keypunch machine and compiler to get my allotted time on the mainframe. I missed my slot and had to start again from scratch.

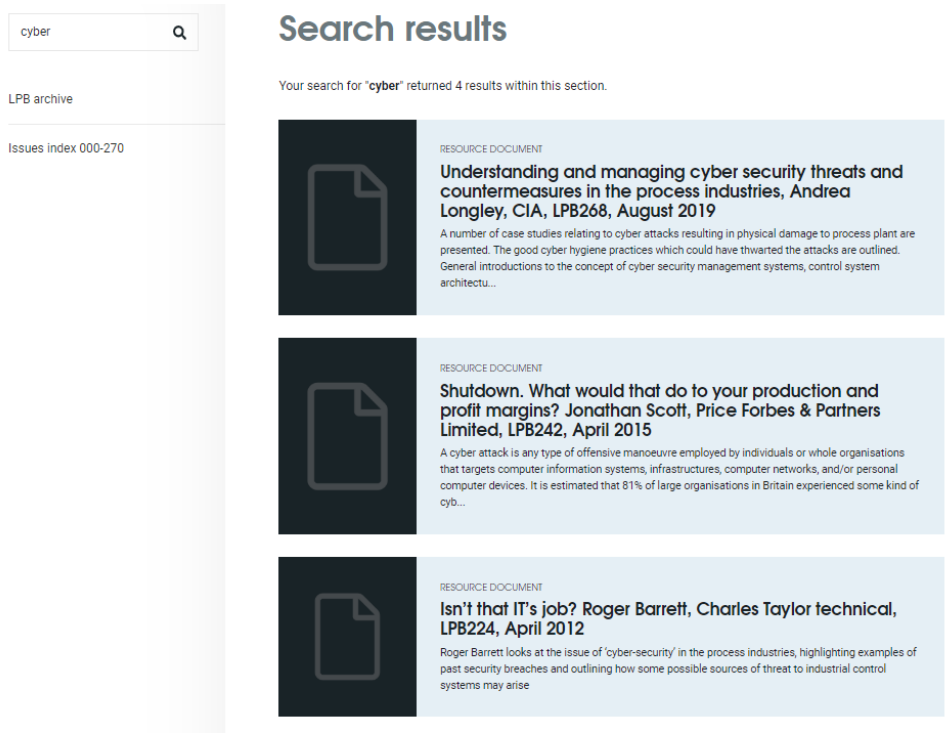


FORTRAN Port-A-Punch card.

In 1988 on being told that all the engineers were being given a personal computer to sit on a desk, I laughed. As a project manager, I no longer wrote Fortran programs or performed complex design calculations that merited such processing power and initially refused the offer. In those distant days, controls were pneumatic 3-15 psi and tuning a process controller involved a screwdriver. I valued my desk space for rolling out A1 sized drawings and schedules. Now, I couldn't live without my laptop and smart phone; the world of work has changed beyond recognition in my working lifetime.

Put the keyword Cyber in the LPB archive.

2 *(Skybrary website accessed 16th January 2020)*



Screenshot from LPB website accessed 16 Jan 2020

Story 1 - Triton

In Greek mythology, Triton was the messenger god of the sea. Son of Poseidon and Amphitrite with the torso of a man and the tail of a cephalopod, he used a conch shell to trumpet his commands and master the sea.

Greek mythology.com accessed 16th January 2020

Triton is also the codename for a sophisticated piece of malware which was used to attack the Safety Instrumented Systems (SIS) at a high hazard process plant in 2017[3]. The attackers took remote control of a SIS control workstation and attempted to reprogram process controllers. In this case, the SIS detected a fault and moved to a safe state. The attack is believed to have been state sponsored, and it is unlikely that a safe (if costly) shutdown of a huge Saudi Arabian oil refinery was the aim. The TRITON attack demonstrates the risk of allowing two-way communication between control and safety systems.

Separating operational technology (OT) environments from information technology (IT) environments – i.e. separation of the industrial automation or plant control networks from general business networks – is essential to cyber security.

But that's not enough. A robust program of cyber assurance must also look at roles and responsibilities, access control, management of change. Cyber competency comes with an understanding of vulnerabilities and failure mechanisms so that appropriate countermeasures can be implemented.

The cyberworld is constantly evolving, and the cyber security response must remain one step ahead.

I leave this section with a question for you. Who has primary responsibility for the cyber security of the industrial control systems in your organisation? Engineering? Maintenance? IT?

If you don't know, I suggest you find out.

2. ENVIRONMENTAL PROTECTION - Natural hazards

Over the five decades of the LPB, authors have drawn attention to the special dangers relating to process plant affected by natural disasters (earthquake, flood, lightning etc.).

Natural event	Country	Year	Main consequences
Landslide	Ecuador	2013	Spill of 1.6 million litres crude oil from a pipeline; the oil entered a river and created transboundary consequences
Hurricane Sandy	USA	2012	Multiple hydrocarbon spills from an oil terminal (>1.3 million litres); 42 billion litres of sewage spilled
Tohoku earthquake and tsunami	Japan	2011	Fukushima nuclear accident; major releases, fires and explosions at several refineries, petrochemical facilities and many other installations
Lightning	France	2011	Tank fire at a hydrocarbon storage tank at a refinery and subsequent explosion
Verdigris River flood	USA	2007	Spilling of 305 m^3 crude oil into floodwaters; release of smaller amounts of petrochemicals and of coke fines
Hurricanes Katrina and Rita	USA	2005	Release of 30 million litres of oil on- and offshore; 113 off-shore platforms destroyed, 163 severely damaged
Low temperature	France	2002	Release of 1,200 tons of cyclohexane due to non-functional heating and low outside temperatures
Elbe River flood	Czech Republic	2002	80 tons of chlorine released from a chemical facility; release of mercury and dioxins
Heavy rain and snow melt	Romania	2000	100,000 m^3 of tailings sludge containing cyanide were released from a breached dam polluting several rivers and resulting in a major transboundary accident
Kocaeli earthquake	Turkey	1999	Major fires at a refinery; release of 6.5 million kg acrylonitrile from a chemical facility
San Jacinto River flood	USA	1994	36,000 barrels of crude oil and 7 billion ft^3 of natural gas were spilled from 8 ruptured pipelines

Table 1: Selected major Natech accidents worldwide over the past 25 years (from the eNatech database). [4]

[3] Understanding and managing cyber security threats and countermeasures in the process industry. Andrea Longley, CIA. LPB 268, August 2019

[4] Natech emergency management – rising to the challenge Apr-17 LPB 254 Elisabeth Krausmann, Amos Necci & Serkan Girgin, European Commission Joint Research Centre (JRC)

Story 2 – in pictures

Figure 1– Fires at a refinery's storage tank farm following the 1999 Kocaeli earthquake in Turkey[6]. International response efforts were required to cope with the emergency

Figure 1 - Destroyed heavy oil tank at a thermal power plant battered by the mega tsunami following the Tohoku earthquake (Photo credit: A. Kouchiyama).

Figure 2 – Hydrocarbon release at a refinery during the Coffeyville floods in the USA in 2007. The flood exceeded the embankments protecting the town by over one metre, eventually causing a release of 400m³ of crude oil that polluted a wide swath of land (Photo credit: Civil Air Patrol).

Figure 4 – Lightning-triggered fire in a gasoline storage tank (Photo credit: Assistant Chief D. Brasuell (ret.), Bixby (OK) Fire Department; Courtesy of Industrial Fire World Magazine).

The recent wild-fires followed by flooding in Australia remind us that such events not only devastate communities, they also destroy the infrastructure needed to contain the disaster: electricity and water for fire-fighting, roads for access and evacuation.

"More hazards due to climate change and growing industrialisation coupled with a higher vulnerability due to community encroachment … imply more… natural hazard triggered technological ("Natech") accidents[5]."

"Natech accidents often feature multiple and simultaneous loss-of-containment events in different locations, creating difficulties for response and effectively increasing the risk of cascading events. Furthermore, the natural hazard can render services necessary for responding to the accident (e.g. water or power) inoperative or inaccessible.[5]"

It is unacceptable to blame accidents on Acts of God. Whether it is required by local legislation or not, active risk mitigations is a condition of our moral licence to operate.

[5] Natural hazard triggered technological (Natech) accidents – an overlooked type of risk? Aug-16 LPB 250 Elisabeth Krausmann, European Commission, Joint Research Centre

3. HUMAN FACTORS - Alarm Rationalisation

Story 3 - Milford Haven (1994)

An overflow of boiling, flammable liquid from an oil refinery flare drum led to an explosion and fire, injuring 26 people and causing £48 million of damage plus major production loss. The incident started with a lightning strike, but a poorly designed alarm system meant that operating staff were overwhelmed with information (and misinformation). The explosion occurred five hours after the initiating event.

The investigation report recommended that

1. Safety critical alarms should be distinguishable from other operational alarms
2. Alarms should be limited to the number that an operator can effectively monitor

Alarms in 10 minutes after major upset	Acceptability
More than 100	Excessive
10 to 100	Hard to cope with
Under 10	Manageable

[6]

It is one thing to know this, quite another to implement the changes needed to fix it. I should know. As the site manager for a high hazard manufacturing facility, I led an alarm rationalisation project based on the excellent EEMUA[7] guidelines.

My experience closely matches that of Bransby and Jenkinson [8]

In normal operation almost half of all alarms were nuisance alarms, repetitive and fleeting, active for less than thirty seconds and of little or no value. In most cases these were eliminated by addressing instrumentation or range settings.

A further class of alarms were the alarms that told the operator what she already knew. If I deliberately stop a pump at the end of a batch, I don't need a flood of alarms to tell me: pump stopped, low discharge pressure, low flow.

The situation worsened, with alarms arriving too fast for the operator to take them in, during an upset. Many of the alarms were not alarms at all, simply information that the Safety Instrumented System (SIS) had done what it was designed to do and closed feed valves and suspended heating. The important alarms that would help diagnose the real problem were lost in the flood and operators repeatedly "accepted" alarms without analysing them.

"… alarm system are often failing badly in their management of the operator's attention … trying to attract his/her attention too often to be effective and doing this with messages that are often irrelevant."

The third point from the Milford Haven investigation report is the one that many people forget. It recommended that

3. Ultimate plant safety should not rely on operator response to a control system alarm

4. SYSTEMS AND PROCEDURES - Management of Change

The size of a change bears no relation to the magnitude of the hazard which may be created[9].

Story 4

A plant was close to commissioning and one of the design process engineers was belatedly informed that the specified catalyst mesh size on a reactor was not available but one slightly larger was. After checking the pellet size against the mesh the process engineer agreed to the change without further review. Unfortunately, the catalyst physically shrank on reduction making it small enough to pass through the mesh where it disintegrated. This resulted in the total loss of catalyst and unplanned shutdowns costing millions of dollars.[9]

[6] Better alarm management December 2001 LPB 162 Tony Ford and Roy Lord*, 4-sight Consulting, *BP Refinery, Coryton

[7] EEMUA[7] 191 'Alarm systems: a guide to design, management and procurement'

[8] How alarming! - Improving the effectiveness of alarm systems Dec-97 LPB 138 Matthew Bransby, Bransby Automation & James Jenkinson, Tekton Engineering

[9] Recognising small plant changes Oct-14 LPB 239 Colin Feltoe, Safety Solutions Ltd

Story 5

Purchasing found a cheaper supplier for a high hazard liquid raw material. It would be delivered to the site's dedicated delivery point in the same type of ISOtank with the same connections. The plant was not consulted, and Purchasing did not raise an MoC. The first delivery demolished the delivery gantry leading to a modest loss of material to the environment but a significant loss of production. The new supplier had a different haulier who used a higher trailer to carry the ISOtank[10].

Corporate reorganization and downsizing bring changes that need careful examination before implementation.

Story 6

Hickson and Welsh Ltd – 1992 A jet fire erupted from a vessel being cleaned, killing five people and injuring 17. A change of company structure had replaced a linear structure with a matrix organisation. One result was that the role of plant manager had been eliminated. An area manager, with support from others, was supposed to have responsibility; however, they had become overloaded and had not been able to provide sufficient attention to planning the cleaning of the batch still.

Story 7

Esso Longford – 1998 A pipework failure caused by low temperature embrittlement allowed gas to release. The resulting explosion and fire killed two people and injured eight; and caused major disruption to the natural gas service for the local population. One of the underlying causes was changing the location of engineers. Previously they had been on site and readily available to deal with queries and concerns, and maintain a degree of oversight. Once they were moved off-site, communication became more formal and focussed, with specific questions being answered by engineers but less general discussion taking place.

Story 8

Bayer CropScience LLC – 2008 A runaway reaction occurred during a plant start-up following a major capital project and resulted in an explosion and fire that destroyed the plant, killing two people and injuring eight. The company had reduced the number of technical advisors it employed without ensuring it retained the necessary knowledge of hazards and risks. One result was that operational input to the capital project was provided by someone with no relevant operational experience of the plant, meaning that the design was not consistent with the existing plant.[11]

If you type 'change' into the LPB archive search you access 70 papers and many more than 70 cautionary tales.

5. SAFETY CULTURE - Corporate memory

"Organisations have no memory. Only people have memories and after a while they move on, taking their knowledge and experience with them.[12]"

A plant manager was quoted as saying[13]

"…there is an `energy conservation principle' in safety. In companies where safety is a value, you will always need to spend significant amounts of time on safety. The choice you can make is whether you spend this time before or after an accident. You can spend time after an accident dealing with the consequences, investigations, lost production, litigation etc. Alternatively, a much more productive and preventative approach is to spend time identifying things that could cause safety problems by paying attention to accidents which have occurred elsewhere, and near misses and safety observations which are local and specific to the plant."

Iqbal Essa HSE & a previous Chairman of Loss Prevention Panel summed up the message from Trevor Kletz

"…organisations and those running them have a duty and moral responsibility to capture and retain within organisational memory the lessons learnt so that others may make better use of them to prevent accidents from happening again."

And this is where the LPB – the process safety memory book for IChemE - can help.

'if you want the present to be different from the past, study the past.' Spinoza 17th century rationalist philosopher.

6. KNOWLEDGE AND COMPETENCE - Case histories

For me, the greatest strength of LPB is the collection of in-depth case studies. If people only see summaries of accidents, they may think – well that couldn't happen to me, here. I'd never be so foolish as to store forty tonnes of methyl isocyanate in a centre of population and switch off all my safety systems. But with almost all major accidents, there are multiple small slips which led up to a major disaster, and for most us in manufacturing, some of those slips will be unpleasantly familiar. You may think you know what happened in Bhopal in 1984, but I will guarantee that if you read the special editions focussing on major accidents in the process industry, you will learn something new, something useful to your current job.

[10] Management of change - what does a 'good' system look like? Jun-19 LPB 267 Ken Patterson & Gillian Wigham

[11] Andy Brazier LPB 239 October 2014 Organisational Change

[12] Inherently safer plant: the concept, its scope and benefits Jun-83 51 Trevor Kletz

[13] " Safety Culture by design" Gonzalo Rios, a Plant Operations Manager, Nomex, Dupont

- Flixborough[14]
- Chernobyl[15]
- Piper Alpha[16]
- Bhopal[17]
- Texas City[18]

The stories that resonate and stay with us, can also be from allied industries. Over many decades, Tony Fishwick has been examining the stories of the less well known accidents and is the most prolific author of LPB papers. Stories that really stick in your mind like the Great Molasses Spill[19] in Boston or the tragedy of the Hamlet chicken processing plant[20] or the mystery of the disappearing lake [21].

7. ENGINEERING AND DESIGN – Inherent Safety

Which brings us to the single most important theme of the conference - Engineering and Design.

Story 5 - Boeing 737 MAX

On October 29, 2018, Lion Air Flight 610, plunged into the Java Sea 13 minutes after taking off from Soekarno–Hatta International Airport, Jakarta, Indonesia. All 189 people on board died. On March 10, 2019, Ethiopian Airlines Flight 302, crashed approximately six minutes after taking off from Addis Ababa, Ethiopia, killing all 157 people on board. Both accidents occurred on brand new Boeing 737 MAX planes and led to groundings across the world.

The full investigation is yet to complete, but it appears that rather than re-designing the aircraft to meet new performance targets, Boeing used an existing aircraft body design and added extra software controls to cope with changes. A Manoeuvring Characteristics Augmentation System (MCAS) introduced new software to compensate for the fitting of heavier engines, automatically forcing the nose of the plane down to avoid stalling.

The alternative to safety by adding belt and braces is inherent safety by design.

Put the keyword inherent safety into the LPB archive search and you find several articles by Trevor Kletz[22], the godfather of Process Safety, who championed the idea of inherent safety for the process industries. They key steps are:

- Minimize

  Reduce the amount of hazardous material present at any one time.

- Substitute

  Replace one material with another of lower hazard

- Moderate

  Reduce the strength of an effect

- Simplify

  Eliminate problems by design rather than adding additional equipment or features to deal with them.

He also emphasised the importance of

- Error tolerance

  Design to withstanding possible faults or deviations from design.

- Resilience

  Limit consequences of failure by design, knock-on effects, incorrect assembly impossible, make status clear.

[14] Nylon Years Apr-19 266 Ramin Abhari
[15] Chernobyl – 30 years on Oct-16 251 Fiona Macleod
[16] Piper Alpha Special Issue LPB 261 June 2018
[17] Bhopal Special Issue LPB 240 December 2014
[18] Lessons from Texas City A Case History Dec-06 192 Michael P. Broadribb, BP America Production Company
[19] A sticky problem – new light shone on Boston's great molasses spillage Dec-18 264 Tony Fishwick
[20] The Hamlet chicken processing plant fire — outcomes and good practices for avoiding a recurrence Apr-18 LPB 260 Tony Fishwick
[21] The Lake Peigneur drilling disaster - small change or minor modification? Jun-19 267 Tony Fishwick
[22] Inherently safer plant: the concept, its scope and benefits Jun-83 LPB 51 Trevor Kletz

- Ease of control

One of the characteristics that made Trevor Kletz such a gifted communicator was his sense of humour.

Cartoon from LPB October 1983

In "**Belt and braces[23]"** he illustrates the diminishing return of adding safety controls to a poor design, in this case male trousers where the waist dimensions are equal to or larger than the hip dimensions of the wearer.

Even if every man with such poorly designed trousers wears 'belt and braces' together, a significant number of men still risk losing their trousers every year due to concurrent failure of both belt and braces.

"At the national level it is considered intolerable that so many men should be embarrassed in this way.[23]"

Of course, there is a simple, inherently safe solution.

Wear a dress or skirt.

macgregorandmacduff and Kikku websites accessed 16 January 2020

[23] Belt and braces, LPB 227, October 2012, Trevor KletzTrevor Kletz and Colin Feltoe

Conclusion

What have we learned and what has changed in 5 decades?

In the 200th paper published in LPB, Robin Turney, then chair of the LPB panel, discussed the changes in process safety between 1974 and 2008. He outlined the interplay between major events and the changes in legislation.

In the 1970's the Health and Safety at Work Act introduced a requirement for UK companies to have a Safety policy. Throughout the 1980's responsible companies developed active Safety Management Systems to implement the policies. The Flixborough accident highlighted how ill-advised modifications to process equipment can invalidate the design basis of safety and the importance of rigorous Management of Change. The Piper Alpha tragedy extended the need for safety cases to offshore operations.

In the 1970's few companies had a rigorous hazard identification process. HAZOP and HAZAN were virtually unknown outside of ICI and although engineers understand the importance of inherent safety by design, this was not always so well understood by accountants. Good front-line managers have always understood their people, but this sensitivity to human factors did not always extend to senior leadership who, when something went wrong, looked for someone to blame.

The renewed emphasis on safety culture and leadership puts responsibility back in the boardroom where it belongs. And Safety-II gives us a new perspective, striving to achieve things that go well rather than by preventing them from going wrong[24].

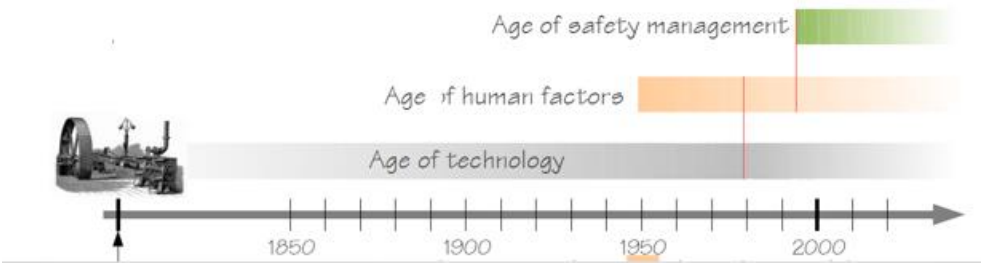
Learning from accidents has never been easier with internet search engines and Wikipedia articles, CSB videos, graphic novels, and the LPB archive.

What has not and will never change?

People don't really change that much. The things that make us brilliant, also make us fallible.

In real work, we face a variety of difficulties, complexities, dilemmas and trade-offs and are called on to achieve multiple, often conflicting, goals (ETTO)[25]. It is practically impossible to provide guidelines or instructions that are detailed enough to be followed 'mechanically.' How work is actually done, how everyday performance is adjusted to match the conditions and why things go well is a prerequisite for understanding what has or could go wrong (WAI-WAD)[24].

And when you investigate accidents, what you look for is what you find. (WYLFIWYF)[24]



1 Hollnagel, E. (2014). Safety-I and Safety-II: The Past and Future of Safety Management. Farnham, UK: Ashgate.

How should we respond?

First ask yourselves seven questions.

1. Do you discuss accidents and near misses suffered by others? (Case Studies)
2. Do you share openly the stories of your own accidents and near misses? (Corporate Memory)
3. Do you assess the process safety implications of all, including organisational, change? (Management of Change)
4. Does any part of your plant safety rely on operator response? (Alarm Rationalisation)
5. What damage could your facility cause if a terrorist gained access to your industrial control systems ? (Cyber attack)
6. And then the emergency services lost road access, communication, power and water? (Natech)
7. And now, does everyone in your senior leadership team understand the importance of Inherent Safety by Design? (ISD)

[24] Hollnagel Sageguard 175 Myths and Misunderstandings
[25] Hollnagel Ref

To paraphrase Judith Hackett [26]

We need leaders who know what they don't know and are willing to learn.

We need leaders who can live with a chronic sense of unease.

We need leaders to give the same priority to process safety wherever they are in the world.

Trevor Kletz described his technique as "…good natured persistence. You have got to keep lobbying and persuading until your job is done."[27]

We need everyone to open the memory book and act on the lessons learned.

Cartoon from LPB 124 August 1995

With thanks to all the LPB contributors, including the most prolific : Andy Brazier, John Bond, John Lundley, Philip Carson, Robin Turney, Terry Gilliard, Tony Fishwick, Trevor Kletz and Vic Marshall.

[26] https://www.hse.gov.uk/aboutus/speeches/transcripts/hackitt221013.htm

[27] Trevor Kletz By accident. A life preventing them in industry. P24