Abstract - The challenge for process industries and chemical engineers is to learn from the past and implement these lessons sustainably into the future. Unfortunately there are many examples, such as Texas City, Formosa, Longford and Deepwater Horizon, where previous incidents within an organisation could have provided valuable lessons in identifying and correcting the hazards which ultimately led to a major incident, if the information had been captured by the Safety Management System (SMS) and used.

An analysis of causes of major incidents over time has shown a change in the nature of major incidents and SMS deficiencies. In earlier major incidents, such as Flixborough, control measures were not in place due to a lack of understanding of potential hazards. This situation has changed with industry identifying the need for control measures, through hazard identification processes, and implementing them. However in later major incidents the control measures, while present, were not sufficiently effective when required to avert a major incident. The SMS had not provided adequate support for these control measures.

Understanding the deficiencies of the past is the first step to improving process safety. Ensuring these deficiencies do not continue is the challenge for tomorrow, which needs to be addressed today.

Key Words: major incidents, safety management system, process safety.

INTRODUCTION

The challenge for chemical engineers, and industry, is to learn from past incidents and ensure these learnings are implemented and remain operational into the future. Kletz (1993:1) commented on this some 20 years ago:

*It might seem to an outsider that industrial accidents occur because we do not know how to prevent them. In fact, they occur because we do not use the knowledge that is available.*

Unfortunately, there are many examples since Kletz’s comment in 1993, such as Texas City, Formosa, Longford and Deepwater Horizon (CSB 2007:103, Hopkins 2008:4, Visscher 2008:42, Dawson & Brooks 1999:15.7 and Hopkins 2011:12), where previous incidents within an organisation could have provided valuable lessons in identifying and correcting the hazards which ultimately led to a major incident, if the information had been captured by the SMS and used (Hale 2003:194 and Koornneef 2000).

Almost every aspect of what went wrong at Texas City had gone wrong before, either at Texas City or elsewhere. (Hopkins 2008:4)

This paper will briefly examine seven past major incidents, highlighting the changing cause of major incidents, and what this means for chemical engineers and the challenge this poses for the future.

MAJOR INCIDENTS – AN OVERVIEW

Hopefully chemical engineers are familiar with some, if not all, of the major incidents which occurred at Flixborough, Seveso, Piper Alpha, Bhopal, Pasadena, Longford and Texas City. They are summarised in Table 1. Before examining what these major incidents indicate about the changing nature of major incidents and specifically control measures over time, a brief overview of each major incident will be provided.

Flixborough

On 27 March 1974 Reactor 5 was leaking cyclohexane and the plant was shutdown (Parker 1975:para 55). A temporary dog-leg bypass was constructed from the 28-inch Reactor 4 outlet to the 28-inch Reactor 6 inlet using 20-inch pipe that was readily available (Lees et al. 1996:A2/5). The three-piece bypass was necessary as the reactors were at different heights (Kletz 1998:56). Bellows were left at each end of the bypass. The bypass piping rested on purpose-built scaffolding (Kletz 1998:57). The plant was started up and operated without incident.

The explosion killed all 18 people in the control room, flattened the main office buildings and started several fires (HSEa, Lees et al. 1996:A2/7). The Flixborough Inquiry concluded:
<table>
<thead>
<tr>
<th>Location</th>
<th>Date</th>
<th>Company</th>
<th>Process</th>
<th>Major Incident</th>
<th>Fatalities</th>
<th>Injuries</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flixborough, UK</td>
<td>1/6/74</td>
<td>Nypro (UK) Ltd</td>
<td>Production of caprolactam</td>
<td>Explosion in oxidation of cyclohexane process</td>
<td>28 workers</td>
<td>36 on-site 53 off-site</td>
<td>Death toll likely to have been higher if it occurred during a weekday(^a) (Parker 1975:para 1).</td>
</tr>
<tr>
<td>Seveso, Italy</td>
<td>10/7/76</td>
<td>Industrie Chimiche Meda Societa Azionara (ICMESA)</td>
<td>Batch production of 2,4,5-trichlorophenol (TCP)</td>
<td>Toxic release of TCDD (2,3,7,8-tetrachlorodibenzo-p-dioxin)</td>
<td>0</td>
<td>477 people reported skin injuries (burns &amp; chloracne)</td>
<td>Environmental damage. 78,000 small animals and 700 large animals were slaughtered to prevent dioxin entering the food chain (Marshall 1987:365).</td>
</tr>
<tr>
<td>Bhopal, India</td>
<td>2-3/12/84</td>
<td>Union Carbide India Ltd</td>
<td>Production of Sevin</td>
<td>Toxic release of methyl isocyanate (MIC)</td>
<td>3,787+ workers and near-by residents(^b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Piper Alpha, UK</td>
<td>6/7/88</td>
<td>Occidental Petroleum (Caledonia) Ltd</td>
<td>Offshore oil and gas processing</td>
<td>Oil platform explosion and fire</td>
<td>167 workers(^c)</td>
<td></td>
<td>Oil platform destroyed and UK hydrocarbon production decreased by 11% (Wells 1997:220).</td>
</tr>
<tr>
<td>Pasadena, USA</td>
<td>23/10/89</td>
<td>Phillips 66</td>
<td>Polyethylene production</td>
<td>Polyethylene plant explosion and fire</td>
<td>23 workers</td>
<td>130 to 300</td>
<td>Nearly US$750 million in property damage - the costliest single owner property damage loss in the petrochemical industry (at that time) (Sanders 2005:98).</td>
</tr>
<tr>
<td>Longford, Australia</td>
<td>25/9/98</td>
<td>Esso Australia Resources Ltd</td>
<td>Gas and crude oil processing</td>
<td>Gas plant explosion and fire</td>
<td>2 workers</td>
<td>8</td>
<td>Gas supply from the plant ceased for several weeks.</td>
</tr>
<tr>
<td>Texas City, USA</td>
<td>23/3/05</td>
<td>BP</td>
<td>Oil refinery</td>
<td>Isomerisation unit explosion</td>
<td>15 workers</td>
<td>180</td>
<td>All fatalities were contractors, located in portables (Visscher 2008:41).</td>
</tr>
</tbody>
</table>

\(^a\) The potential death toll estimated at 128 if the explosion had occurred during the week with the offices occupied (Kletz 2001:86).

\(^b\) The exact death toll was never clearly determined (Marshall 1987:373). Lees et al. (1996:A5/9) estimates the death toll at 2,000, Willey et al. states the official documented death toll as 3,787 with an estimated undocumented death toll of over 10,000 (Willey et al. 2006:1), while Lapierre & Moro (2001:366) estimate the death toll between 16,000 and 30,000 people.

\(^c\) Including 2 rescue crewmen from a support vessel.
The disaster was caused by the introduction into a well designed and constructed plant of a modification which destroyed its integrity. The immediate lesson to be learned is that measures must be taken to ensure that the technical integrity of plant is not violated. (Parker 1975: para 209)

Design and manufacturing deficiencies of the dog-leg bypass were identified (Parker 1975: para 61-63, 68, 72). ‘There was no overall control or planning of the design, construction, testing or fitting of the assembly nor was any check made that the operations had been properly carried out’ (Parker 1975: para 71). The investigation showed a clear failure of the change management process. Other factors contributed to the number of fatalities, including plant congestion, which increased explosion pressures, and vulnerability of the control room (Parker 1975:para 218).

Seveso

On 9 July 1976 at 4pm a TCP batch was begun, reacting 1,2,4,5-tetrachlorobenzene and caustic soda, in the presence of ethylene glycol (Lees et al. 1996:A3/6). TCDD (2,3,7,8-tetrachlorodibenzo-p-dioxin), the most toxic chemical in the dioxin family, is an undesirable by-product, which is minimised (1ppm of TCP) by maintaining the temperature below 180°C (Lees et al. 1996:A3/3). Prolonged heating of the reactor at 230-260°C can increase TCDD production a thousand-fold (Lees et al. 1996:A3/3). Normally 50% of the ethylene glycol is removed, however only 15% was removed on 9 July, and the process interrupted (Lees et al. 1996:A3/7). Heating stopped, however water was not added to cool the batch to the specified 50-60°C and the temperature recorder and agitator were turned off (Lees et al. 1996:A3/3). The plant was then closed for the weekend as required by Italian law, with the batch left in the reactor (Kletz 2001:104). The steam turbine was on reduced load, as required by Italian law, with the batch left in the reactor (Kletz 2001:104). On 10 July the bursting disc on the reactor ruptured, sending a dense cloud of toxic chemicals several kilometres from the plant (Kletz 2001:103).

The investigation concluded the Seveso incident was the result of design and operational failures. Plant activities were contrary to operating procedures (Wells 1997:6). The design allowed toxic liquid to be discharged direct to the atmosphere and the reactor had an unnecessarily hot heating medium (300°C steam) with a runaway reaction possible at 230°C (later revised to 185°C) (Kletz 1998:376). Fundamentally these design deficiencies can be traced back to a lack of understanding or identification of the hazards. Kletz (1998:217) reports that:

- a catchpot after the relief device would have prevented the reactor contents from reaching the atmosphere.
- No catchpot was installed as the designers did not foresee that a runaway [reaction] might occur, although similar runaways had occurred on other plants.

Bhopal

Methyl isocyanate (MIC) was an intermediate product in the production of Carbaryl, the active ingredient in the pesticide Sevin (Wells 1997:204). MIC is unstable, requiring storage at low temperatures (Bowonder & Miyake 1988:240). At Union Carbide India Ltd’s Bhopal facility, there were three refrigerated underground MIC tanks (Wells 1997:204). The plant was not originally designed for MIC (Wells 1997:204), with on-site production of MIC commencing in 1979 (Lees et al. 1996:A5/2).

By 1983, decreasing profits coupled with the departure of experienced engineers, saw the plant’s level of safety decline (Bowonder & Miyake 1988:240). Manning levels and the maintenance crews were cut (Marshall 1987:378). Chouhan (2005:206), an employee of Union Carbide India, reports the MIC refrigeration unit was shutdown in May 1984 and its refrigerant removed, despite the storage tanks still containing MIC. The vent gas scrubber, on the vents of the MIC tanks, was also inoperable due to maintenance and reportedly low levels of caustic soda (Ayres & Rohatgi 1987:24). The flare tower was under maintenance, however it was not completed due to staff shortages (Chouhan 2005:207).

On the night of the incident, pipework in the MIC plant was flushed with water, without the necessary isolations (Chouhan 2005:207). Isolations were previously performed by the maintenance department which had suffered heavy redundancies several days prior (Wells 1997:205). It is hypothesised that flushing water entered a MIC storage tank, resulting in a runaway reaction, causing discharge of MIC to the atmosphere (Bowonder & Miyake 1988:244, Chouhan 2005:205 and Kletz 1998:368). Forty-one tonnes of MIC discharged through the tank’s relief valve in two hours (Willey et al. 2006:1).

Management decisions had disabled many control measures, which would have prevented or reduced the consequences of this incident (Chouhan 2005:206 and Wells 1997:205). Mitigation controls were also ineffective, for example water sprays only reached a height of 15 m, yet the MIC was released at 33 m (Chouhan 2005:206, Marshall 1987:378 and Wells 1997:205).

MIC was an intermediate product in the production of Sevin and the storage of such large quantities was unnecessary. The most important lesson from Bhopal being ‘What you don’t have, can’t leak’ (Kletz 2001:111), which is now a key concept in inherent safety.

---

1 Marshall (1987:377) reports there is controversy regarding the operational status of the scrubber.
Piper Alpha

Piper Alpha was an oil and gas platform in the North Sea operated by Occidental Petroleum (Caledonia) Limited (Kletz 2001:196). Three other platforms pumped hydrocarbons to Piper Alpha for distribution to Flotta, Scotland (Wells 1997:220). At the time of the incident, the platform was undergoing maintenance (Lees et al. 1996:A19/7). A decision to completely shut down the platform for maintenance was overturned, continuing limited production (Cullen 1990:235).

One of two condensate pumps, Pump A, had its relief valve removed for maintenance (Wells 1997:221). At shift hand-over, the night shift was incorrectly informed that Pump A was operational (Wells 1997:221). Pump B was fully operational. Around 9.45pm Pump B tripped and could not be restarted (Cullen 1990:71-72). Pump A was re-instated, requiring electrical de-isolation (Lees et al. 1996:A19/7).

Three low level gas alarms sounded, followed by a high level alarm at 10pm (Cullen 1990:74). An explosion in the pump area killed several workers (less than 10) and destroyed the platform’s fire-fighting system (Wells 1997:221). The resulting fire engulfed the control room, damaging the platform’s communication systems (Lees et al. 1996:A19/8).

The other connected platforms continued to feed hydrocarbons to Piper Alpha for over an hour (Wells 1997:221). This led to further explosions and a large number of fatalities (Cullen 1990:138-145). The helicopter evacuation drill was followed by some, however smoke and flames prevented the helicopter’s approach (Cullen 1990:2).

The platform was destroyed within two hours (SIA 2008). One hundred and sixty-seven personnel died – 62 people survived (Lee et al. 1996:A19/2). Most fatalities were caused by smoke inhalation in the galley (the muster point) and accommodation areas (Kletz 2001:197 and Wells 1997:221).

The investigation found a series of procedural non-conformances had occurred during maintenance activities on Pump A. The supervisor, who was a contractor, had not received training in the permit to work (PTW) system. Furthermore the shift hand-over did not adequately cover the maintenance work on Pump A. The design of the platform and its emergency protective systems did not provide protection against major incidents. The lack of emergency planning for such a scenario, and communication problems resulted in the continued supply of hydrocarbons to Piper Alpha. The cessation of hydrocarbon supply would have reduced the consequences of the incident.

This incident occurred during simultaneous operations of maintenance and production. The Inquiry was critical of this management decision. The pressure on personnel to continue production was also considered a contributing factor to the incident.

The deficiencies on Piper Alpha were failures in systems. Either there was a system but it was inadequately designed and executed, the PTW system, or there was no system where one should have existed, for example, the lack of a systematic method for assessing major hazards or the lack of a system for training in inter-platform emergencies. (Kletz 2001:205)

Pasadena

Phillips 66 produced high-density polyethylene in the Houston Chemical Complex in Pasadena (OSHA 1990:vii-viii). Polyethylene is formed via the polymerisation of ethylene in isobutene at high pressure and high temperature (Wells 1997:9). Polyethylene particles settle out and are removed from the tall vertical reactor in settling legs (Lees 1996:A6/2).

Maintenance work began on Reactor 6’s settling legs (HSEb). To isolate the settling leg from the reactor, maintenance procedures required isolation of a valve and removal of compressed air hoses (Sanders 2005:99). Settling leg Number 4 was isolated and partially disassembled, however a plug of polyethylene was unable to be dislodged (Lees 1996:A6/2). Assistance was sought from the control room and shortly thereafter approximately 85,000 lb of ethylene, isobutene, hexane and hydrogen were released (OSHA 1990:viii). The vapour cloud ignited and exploded, registering 3.5 on the Richter Scale (Sanders 2005:98) and destroyed the sprinkler system (Yates 1990:5). The incident command centre was damaged, disrupting telecommunications and fire systems were severely compromised (Tweeddale 2003:402).

The incident investigation concluded the release occurred because of reliance on isolation by a single air-operated ball valve, which was then inadvertently opened as the valve’s air hoses had been cross-connected due to poor ergonomics (Tweeddale 2003:402 and Welch 1993:243). The isolation used was against company written procedures and standard industry practice (HSEb), which required a double block system or a blind flange (Lees et al. 1996:A6/2).

The Occupational Safety and Health Administration (OSHA) (1990:70) concluded ‘the primary causes of the accident were failures of the management of safety system’ and stressed that ‘Above all, the actions proposed in this report underscore the urgent need for increased attention to established principles of process safety management’ (OSHA 1990:72). The Phillips 66 Company was fined US$4 million by OSHA and was required to institute process safety management procedures at Pasadena, and three other facilities, as well as train Phillips employees and on-site contractor employees about potential hazards (OSHA news release 91-416, August 22 1991).
Longford

The Esso Longford gas plant was built in 1969 and processes gas and crude oil from a number of off-shore platforms into natural gas, LPG and stabilised crude oil, which are exported via pipeline (Dawson & Brooks 1999:11). The Longford gas plant was the sole supplier of natural gas to the state of Victoria (Kletz 2003:54).

A process up-set during normal operation occurred, leading to the tripping of a lean oil circulation pump (Kletz 2003:54). The pump was not restarted for some hours, resulting in a lack of heating medium to several vessels (Kletz 2001:268). These vessels still received a cold fluid and with no heat exchange occurring with the hot lean oil, the vessels dropped in temperature to -48°C, causing embrittlement of the vessel’s steel shell (Dawson & Brooks 1999:3.49). The pump was eventually re-started and the introduction of hot lean oil resulted in brittle fracture of the vessel, causing the vessel to rupture creating a hole greater than 1m diameter with a pressure of 2800 kPa behind it (Dawson & Brooks 1999:5.61 and 7.2). An estimated 10 tonnes of hydrocarbon vapour was released from the vessel, travelling approximately 170 m to the fired heaters where it ignited, causing an explosion and fire (Dawson & Brooks 1999:7.3). An estimated further 10-15 tonnes of hydrocarbons were consumed in the explosion and fire (Dawson & Brooks 1999:7.6).

Due to the location of the failed vessel and the layout of the plant, the three gas plants at Longford were shutdown (even though only one gas plant had sustained damage) (Dawson & Brooks 1999:1.9). Gas supplies to Victoria were stopped, with full supply not being re-instated until some 20 days after the incident (Dawson & Brooks 1999:1.9).

The Royal Commission identified many SMS (known as ‘OIMS’ at the Longford plant) deficiencies. Analysis of these SMS deficiencies (Sinclair 2012:69) indicated all SMS deficiencies were in implementation, with many deficiencies also in measurement and evaluation and/or management review. The Royal Commission found that OIMS elements were either defective or not implemented and ‘reliance placed by Esso on its OIMS for the safe operation of the plant was misplaced. The accident on 25 September 1998 demonstrated in itself, that important components of Esso’s system of management were either defective or not implemented’ (Dawson & Brooks 1999:13.42).

Texas City

The BP Texas City facility was the third-largest oil refinery in the United States, producing 10 million gallons of gasoline per day and other fuels (CSB 2007:17 and 31). On 23 March 2005, the raffinate splitter tower was being restarted after maintenance. During the start-up, liquid hydrocarbons were pumped into the 52m tower without any liquid being removed (CSB 2007:21). The tower was overfilled, causing liquid to enter the overhead piping, which was protected by pressure relief valves (PRV) located 45m below the top of the tower (Visscher 2008:40). As pressure increased, the PRVs opened, discharging a large amount of hydrocarbon to a collection vessel that was open to the atmosphere via a 34 m vent stack (CSB 2007:21). The result was a ‘geyser-like release’ from the vent stack (CSB 2007:21). The hydrocarbon vapour cloud ignited (ignition source believed to be an idling vehicle about 8 m from the collection vessel) and exploded, killing 15 people. These victims were contractors working in temporary offices (portables) located 37 m from the collection vessel (CSB 2007:22).

The U.S. Chemical Safety and Hazard Investigation Board (CSB) revealed that start-up procedures had been violated (CSB 2007:18). Procedures had become ‘outdated documents to be used as guidance’ (CSB 2007:73). Critical alarms and instrumentation were inaccurate and ineffective (CSB 2007:18). The absent Day Supervisor was not substituted by personnel with relevant experience (CSB 2007:86-87). The blowdown system, installed in the 1950s, was an unsafe design; having never been connected to a flare system to safely collect liquids and combust flammable vapours released from the process (CSB 2007:18). Miscommunications occurred among management, supervisors and operations personnel including whether or not the unit was going to be started, how liquid raffinate was to be sent to storage, and the liquid raffinate level in the unit at shift change (CSB 2007:79).

The CSB investigation concluded ‘The Texas City disaster was caused by organizational and safety deficiencies at all levels of the BP Corporation’ (CSB 2007:18) with ‘serious management safety system deficiencies that allowed the operators and supervisors to fail’ (CSB 2007:71). ‘While most attention was focused on the injury rate, the overall safety culture and process safety management (PSM) program had serious deficiencies’ (CSB 2007:19).

The Changing Cause of Major Incidents

What do these major incidents indicate about failures over time? Investigations into all of these major incidents support the widely held (Perrow 1984, Reason 1990, 1997, Kletz 1998, 2001, Lees et al. 1996, Hale 2003, Hopkins 2000, 2008 & Qureshi 2007) view that: industrial accidents are the end-results of long chains of events that start with decisions at management level. Often these decisions create latent failures, which may remain hidden for a long time. (Wagnaar, Hudson & Reason 1990:273)

These major incident investigations also indicate a change in SMS failures over time. Flixborough (1974) and Seveso (1976) indicate that the necessary control measures were not in place to prevent a major incident – often due to a lack of management and technical foresight and knowledge. The possibility of a major incident had not been considered and
hence the SMS did not drive hazard identification, safety assessment or control measure activities to prevent or mitigate major incidents.

_He [Mr Brenner, the Safety & Training Manager at Nypro Ltd, Flixborough] had created a proper system for dealing with normal hazards and was in the course of preparing and putting in hand a disaster plan...it was not designed to deal with an instantaneous catastrophic disaster such as occurred._ (Parker 1975: para 194)

As the hazard of large, or unnecessary, inventories of chemicals had not been recognised prior to Flixborough, ‘little thought’ was given to ways of reducing these inventories (Kletz 1998:368). This was also the case at Bhopal.

While there were design deficiencies at Bhopal (1984), such as the unnecessarily large storage of an intermediate chemical (Kletz 2001:111), the control measures (both preventative and mitigative) were in place such as refrigerated storage tanks, scrubber, flare, etc. (Bowonder & Miyake 1988:240 and Chouhan 2005:206), indicating an understanding of the potential hazards. However, none of these control measures were effective. In fact some had been knowingly disabled, such as the refrigeration system and flare (Ayres & Rohatgi 1987:24). Even if the controls had been active, there is considerable doubt as to their ability to cope with the extent of the major incident scenario, which had not been considered in their design (Marshall 1987:378).

Since Bhopal, investigations into the cause of major incidents have shown that control measures were often in place (suggesting an increase in the knowledge and understanding of hazards), however these control measures were ineffective due to deficiencies in the implementation, operation and/or maintenance of the SMS, including a lack of consideration for major incident potential. An example of this is the erosion of procedural requirements such as the permit to work and shift handover on Piper Alpha (1988) and at Pasadena (1989).

_...the Phillips 1989 explosion...demonstrates the need to adhere to operating procedures and implementing appropriate management systems for contract workers._ (Anthony & McKetta 2001:169)

Further analysis (Sinclair 2012) has shown that in all seven of these major incidents there was a weakness in management review and evaluation activities to critically identify deficiencies and rectify them.

Major incident investigations have developed over time to consider failures of the organisation, through the management system, rather than of the individuals involved (Wreathall & Reason 1992:448, Hale 2003:185). Kletz (2001:267) acknowledges this shift in focus, reporting that the Longford Royal Commission Report ‘describes the operator failings that led to the explosion but does not blame the operators, as reports in earlier times might have done, but shows how the operators’ failings were the result of inadequate training and other management failures’. IOSH (2003:25) reports a greater emphasis on worker and management behaviour in incident analysis. Kletz (2001:271) warns of the limitations of SMSs and highlights the connection between people and systems:

_All that a system can do is harness the knowledge and experience of people...Knowledge and experience without a system will achieve less than their full potential. Without knowledge and experience a system will achieve nothing._

The interaction of people and systems must be considered. This was highlighted throughout the Longford Royal Commission Report. The Longford plant was equipped with many sophisticated process control devices, with alarm systems to alert personnel when any part of the system was operating outside of the parameters set for its operation. Many of these control and alarm devices were rendered ineffective, contributing to a very hazardous situation, due to systemic failure by Esso over some years to manage its own systems efficiently and effectively. ‘There was no evidence that any system existed at Longford for the regular monitoring of operating conditions or operator practices.’ (Dawson & Brooks 1999:13.88). This situation was particularly serious in human terms due to an ongoing failure to manage, supervise and train plant supervisors and operators. The reality was that supervisors and operators were ignorant of the potential dangers involved in operating the plant outside its design parameters, especially in regard to abnormally low temperatures and a failure to understand the existence of metallurgical conditions and brittle metal risk associated with very low temperatures (Dawson & Brooks 1999:13.18). Esso was also heavily criticised for the lack of a HAZOP study on Gas Plant 1 (Dawson & Brooks 1999:15.7).

Many Major Hazard Facilities (MHFs) focus on engineering and hardware at the expense of ‘people’ issues (Anderson 2004:703). Anderson stresses the need for human factors to include process safety aspects of controlling major hazards, such as connecting the wrong hose or omitting components (as occurred at Pasadena), rather than the traditional focus of human factors on personal safety. Part of the human aspect of controls is that all personnel involved must understand the nature of the hazards in their control and the possible magnitude and implications of a major incident. The challenge is to sustain this individual awareness and commitment when incidents fade from people’s memories (Environment Canada 1986:3).

The analysis of major incidents over time suggests that industry is moving from not having control measures in place, due to a lack of understanding of the potential
hazards, to recognising the need for control measures and putting them in place. However in later major incidents the control measures were not sufficiently effective when required to avert a major incident.

**Deterioration of Safety Systems**

The incidents examined illustrate that the design intent of safety systems can be forgotten over time, operations can deviate from procedures, a lack of appropriate maintenance can reduce safety system effectiveness and near misses are often not acknowledged. The need to harness and use knowledge from design, operation, maintenance and past incidents is paramount in processing plants. Flemming and Lardner (2002:2) state:

> ...good systems, procedures and engineering controls on their own are not enough, it is how well an organisation 'lives' its systems that matters.

The Baker report (2007:i), following the 2005 Texas City Refinery incident states:

> The passing of time without a process accident is not necessarily an indication that all is well and may contribute to a dangerous and growing sense of complacency. When people lose an appreciation of how their safety systems were intended to work, safety systems and controls can deteriorate, lessons can be forgotten, and hazards and deviations from safe operating procedures can be accepted. Workers and supervisors can increasingly rely on how things were done before, rather than rely on sound engineering principles and other controls. People can forget to be afraid.

These sentiments are echoed by Tweeddale (2003:xiv) and Kletz (1993:1). Ackroyd (2008:787) comments that the Baker Report (2007) has 'highlighted ...how degradation [of OHS management arrangements] can readily occur even in ‘mature’ organisations’. Gradual degradation in organisational performance, or organisational drift, is often unnoticed (Berman & Ackroyd 2006:140). Long before organisational drift becomes apparent, precursors to incidents are generated (Berman & Ackroyd 2006:149). ‘Practical Drift’ is the gradual deviation, from safe operating procedures, by individuals (Snook 2000). The management of organisational drift is a challenge for detection, as most organisations have well-developed processes for managing and enhancing occupational health and safety (OHS) once the deterioration is brought to their attention (Berman & Ackroyd 2006:150). However, ‘Plenty of examples exist...where the gradual erosion of safety performance appeared never to breach a threshold of organisational consciousness, until a major incident or near-miss made everyone sit up and take notice’ (Berman & Ackroyd 2006:140).

**The Challenge for Chemical Engineers**

Major incidents do demand our attention. Analysis of these major incidents highlights the need for chemical engineers to continue the important task of hazard identification, followed by safety assessment and control measure review to ensure control measures are appropriate to protect against the identified hazard. However our job in preventing major incidents does not stop at hazard identification. The challenge for chemical engineers and industry is to ensure the control measure continues to be effective throughout its operating life, so that if, or when, it is required, its effectiveness can be guaranteed.

Research of Victorian MHFs (Sinclair 2012) reflects the underlying themes of the seven major incidents reviewed here, that SMS implementation levels when critically examined by the safety regulator are often less than expected by the MHF (Sinclair 2012:172) and that this is accompanied by less than optimal control measure implementation results. Further decreases in SMS and control measure operability and auditing data were observed, suggesting MHFs are better at identifying the need for a control measure (following hazard identification processes) and implementing it, than actually checking that the control measure is achieving its intended purpose.

Operability deficiencies indicate that the day-to-day operation of the control measure is being compromised and hence the barrier it provides between the hazard and major incident is not complete. Research (Sinclair 2012:168) has shown significant weakness in industry’s internal auditing practices and the ability to self-identify deficiencies. These results indicate that many SMSs were operating at a less than optimal level, possibly giving the operator a false sense of safety thinking their SMS was implemented, while not being aware of its lack of operability. These results suggest the presence of latent failures (as described in the Swiss Cheese Model (Reason 1997:9)) as should a control measure be called upon in an emergency, its level of operability cannot be guaranteed due to failures in the operability of the SMS element that should be supporting it.

These findings, together with knowledge of past major incidents, should be a wake-up call to chemical engineers and industry to ensure deterioration in safety systems are a key focus of management and are detected with the aim of preventing a major incident.

**Conclusions**

Analysis of seven past major incidents has shown the changing nature of causes from not understanding the hazards, through to understanding the hazards but not having control measures in place which were effective. This was due to deficient SMSs. The analysis of major incidents and the increasing shift away from blaming individuals to finding fault in the management system, suggests a need for organisations to better understand their SMS and how it can
work effectively to prevent defects and deterioration in the control measures (or barriers) which stand between hazards and a major incident.

A key learning from major incidents is that chemical engineers need to understand safety management systems. They need to understand how a specific control measure is managed by the safety management system and determine if this is adequate. They need to appreciate the interaction between people, plant and systems and consider human factors. Chemical engineers need to appreciate the need for hazard identification (including major incident potential) and realise that risk management does not end there. Safety assessment of the identified hazard, followed by control measure review is also important. But this is not a once every five years task; monitoring control measure effectiveness to ensure control measures provide the ongoing protection, which has been assumed in initial design and control measure reviews, is critical. Industry must develop the ability to self-identify gradual safety performance deterioration to prevent major incidents. Ensuring control measures are effective when required in an emergency, is the challenge for chemical engineers and industry.

REFERENCES


Hopkins, A. (2008), Failure to Learn: the BP Texas City Refinery Disaster, CCH Australia, Sydney.


Kletz, T. (1993), Lessons from Disaster – How Organisations have no Memory and Accidents Recur, Institution of Chemical Engineers, Rugby.


OSHA (1990), The Phillips 66 Company Houston Chemical Complex Explosion and Fire, A Report to the President, U.S. Department of Labor, Occupational Safety and Health Administration, Washington, D.C.


Wells, G. (1997), Major Hazards and Their Management, Institution of Chemical Engineers, Rugby.

