The Questions of Recurring Incidents; Why and How to Stop Them?

Ian R. Clarke

Senior Risk Engineer, Swiss Re Corporate Solutions, London, UK

ian\_clarke@swissre.com

1. Introduction

In the insurance industry we spend a lot of money paying claims for incidents, that on paper, look remarkably similar to what has gone before. We, being the risk engineering component of this insurance community, visit clients regularly and conduct risk engineering surveys. During these we talk about process safety leadership, operational discipline, operations and integrity management systems and a host of other systems and processes which we try to examine and critically assess for efficacy. There is little doubt that there are numerous moving parts to this discussion, but I want to focus on just one.

The topic for this presentation is competency validation, or, more accurately, how to try and ensure the operator at the sharp end of the process does what you want him to do, every time. Whether it is during standard operations, which is relatively simple, through to an emergency situation, which is more difficult. There are undeniably a host of organisational factors that influence operator or technician behaviour in an emergency situation, such as the safety culture, leadership directives both communicated but also implied by actions rather than policies, and the organisational structure that determines whether said operator or technician is afforded both the time, resource and degree of empowerment necessary to make the correct decision. We are not going to touch on these issues.

Instead, through a series of ultimately preventable events, we will examine how to try and improve the chances of the right outcome being achieved. Putting aside the organisational factors, which we know play a significant, indeed the most significant, role, how do we improve the knowledge, training and ultimately the decision making of the person at that sharp end? More importantly, how do we validate that we have done it and retained a level we are happy with year on year? All too often we go to sites where the success of the operator training programme is measured by the number of training sessions the client has run, not whether we have actually improved the likelihood of the operators and technicians going home safely. All too often we measure quantity, but not quality.

2. Methods

This is not going to be a description of a competency validation programme, as I am not an expert in that field. After over thirty years in insurance, most of it in the downstream oil and gas arena such as refineries, petrochemical plants, gas plants, ammonia and ammonia based fertiliser plants and tank farms, the only thing I consider myself an expert in is process safety and risk assessment.

However, in recent years we have begun to tackle the question of loss analysis and learning from losses. As many would know, this is a difficult topic to cover in the public arena as not all losses are investigated in that domain, and many losses we see in the insurance industry we investigate on the basis of loss adjuster reports which cannot be shared in the wider environment. This point is amply demonstrated by several instances in this paper where I have used losses from our own internal claims database to illustrate a point, while protecting the anonymity of the client.

However, we do have loss information in the public domain. Some are studies of large losses (Marsh, 2024), some are numerical analysis of large losses (Lloyds Market Association (LMA), 2015), and of course we have the excellent loss reports issued in the public domain by various regulators, the most well known probably being the US Chemical Safety Board (CSB), some of whose reports I will use to illustrate points in this paper.

If you spend any time at all studying losses in our industry one of the first things that becomes apparent is that there is very rarely anything new to learn, especially these days. Losses typically follow one of many well known paths, with contributing factors that are all too familiar to all of us. This begs the question – Why? Why does it happen? Why do the same causes and contributing factors appear again and again, despite our best intentions? Despite what some of my colleagues in the insurance market might think, nobody, well almost nobody, goes to work on a given day with the intention of causing a major catastrophe which may kill themselves or their fellow workers and cause irreparable damage to their workplace and possibly the public and environment. So, why?

Unfortunately there is no single answer to the question of why the same losses occur, but it certainly can be argued that most of these losses are in no way different to what has come before. Like the causes and contributing factors, the answers are very rarely new either. Now the first point to make, which is a very valid one, is that virtually all these losses have organisational and/or design components which are the main reasons for why they occurred. I will present later statistics that show the vast majority of incidents that would fit under an operational heading, rather than asset integrity based failures, occur during transient conditions, such as start ups, shut downs or emergency situations. There are a wide range of things that influence operator behaviour in an emergency such as the safety culture of the facility and the leadership directives which are both communicated formally through policies and those implied by actions. Their behaviour is also influenced by the organisational structure and how emergency situations are managed, plus by the availability of the time, resource and level of empowerment to come to the correct decision. There is plenty of theory and, I'm sure, numerous papers on process safety leadership and culture at this very conference.

The various process safety management system elements that we have become used to seeing are designed to identify the hazards and build a framework of systems and procedures that control them. However, frequently these systems can be used to justify existing levels of controls, avoiding capital spend on technological hardware based solutions which may improve the management of the hazard. As an example, one of the things we look for in Process Hazard Analysis and Hazard and Operability studies (PHA/HAZOPs) is whether credit is taken for human interventions. Anything that is a single operator error away from disaster, you are pushing your luck and potentially putting people in harm's way. Again, I am sure there will be a host of presentations at this conference around improving these systems and procedures.

What I want to concentrate on is improving our very last, or what should be our very last, line of defence, the operator. I accept that the organisational, hardware and software (in this context, management systems) deficiencies on the facilities we operate are the main causes of loss, and I urge everyone to learn lessons from the following losses, including how to make this last line of defence as resilient as possible. Because while most of the losses I am going to use as examples have a myriad of organisational, hardware and software causes, it doesn't alter the fact that if the operators had behaved differently, they may not have happened.

3. Incidents

3.1 Potential Commonality Problems

The first type of incident I want to highlight is the honest mistake made by operators where design provides us with a significant opportunity to make such a mistake. The loss in question occurred on an ethylene cracker unit when an operator opened the wrong manual blind valve on the furnace charge deck, leading to a flash fire. These blind valves were installed to allow the ethane feed lines to be blinded and isolated without the need for opening flanges. The plant in question had 16 cracking furnaces and the valves were located on a series of common charge decks each serving two of these furnaces. The ensuing fire damaged steelwork supports, electrical and control systems, instrumentation and piping throughout the unit, and all furnaces suffered some damage to tubes and refractory due to the thermal shock.

The operators were preparing to shut down one furnace for decoking and start up the adjacent one. During the activity a flash fire occurred. The control room operators immediately activated the water drench systems but the two operators on the charge deck suffered serious burns before being evacuated. The plant was safely shut down and depressurised, with fire fighting efforts beginning almost immediately, preventing fire spread to other areas of the plant. As the manual blind valve on the operating furnace was open following the incident, and there was no reason for it to be so, it was concluded that the fire was caused by a release from this valve.

This loss shares some similarities with the Formosa polyvinyl chloride (PVC) plant explosion which occurred in Illinois some ten years earlier, although the damage was in this instance much more severe. The similarities in the layout between the groups of four reactors within the reactor building, which housed all 24 reactors, led to an operator inadvertently opening the lower drain line on an operating reactor (D310) instead of the one that was being cleaned (D306), despite him having to defeat an interlock to do so. The figure (Figure 1a) on the next page, from the CSB report, shows a diagram of the arrangement. A large cloud of vinyl chloride monomer (VCM) was released into the building and subsequently ignited. Four operators were killed and another died two weeks later. The resultant fire and smoke required roads to be closed and 150 people evacuated. The plant was destroyed and was never rebuilt.

There were a large number of extenuating circumstances as follows:

* The operators were on two levels with no means of communication, so the upper level operator, who controlled the batch system instrumentation, could not speak directly to the operator on the lower level
* The previous owner installed an overpressure safeguard, allowing reactors to vent into adjacent empty reactors to relieve pressure. However, there were interlocks installed on the lines to prevent the valves from being opened if the system was live. Under the previous ownership circumventing this interlock could only be done at the supervisor level, the entire layer of which were removed by Formosa to reduce costs
* As can be seen from the diagram (Figure 1a), the layout was the same for each group of reactors, so a mistake was more likely even given all reactors and consoles were labelled
* There had been a number of previous near misses, and the previous operator had recommended upgrading the interlock system in a PHA some years prior. However, the plant was sold and Formosa had not revalidated the PHA prior to the incident. The PHA, in any event, did not cover transient operations such as cleaning and returning to service

In order to try and prevent incidents of this type, we encourage the following safeguards:

* A brief, pre-task meeting, similar to the "toolbox talk" or job safety analysis (JSA) discussion that would occur prior to a maintenance activity
* Ideally, implement Safety Critical Task Analysis (SCTA). Using the instance of the blind valve above, any hydrocarbon system which requires potentially opening it to atmosphere should be covered by this activity. The subsequent analysis will identify a need for increased training, signage and the like
* Transient operations should be covered by checklist type procedures with every step initialled and, ideally for the most hazardous activities, verified by a second operator
* Note signage is not always a cast iron guarantee (as the Formosa loss showed)
* Increased training refers to effective training, rather than leaving operators to refamiliarize themselves with procedures once every few years. For training to be effective, it requires field validation and testing, and then drills/exercises. Most plants drill only for emergency situations. The best plants will carry out drills not only on emergency situations but also transient operations like switching, reactor changes for cleaning, etc. They will also carry out drills leading up to start ups, covering the different conditions and hazards occurring during these operations, and similarly shut downs. Attendance should be documented and understanding should be confirmed by testing
* Effective training is not sitting the shift in a room, reading through the procedure and getting everyone to sign a piece of paper confirming their attendance

3.2 Hazard Awareness

The second type of incident to discuss are those exacerbated by a lack of hazard awareness. This one is more difficult to address as there is corporate hazard awareness and individual hazard awareness. It goes without saying that individuals can suffer from a lack of hazard awareness, and that this should be addressed by training, upskilling, etc. However, if the organisation itself suffers from a lack of hazard awareness, then that is a different thing entirely. Also note here I am referring to a genuine lack of awareness, rather than conscious decisions to put profits before safety.

An explosion at an ONGC gas plant in India in 2019, which occurred during torrential monsoon rain, showed a lack of hazard awareness throughout the organisation. The ensuing explosion caused massive damage to the plant, as well as four fatalities. The enquiry report (PNGRB, 2020) identified a number of contributing events, including those below:

* The event occurred during the monsoon, and indeed the amount of rainfall was a major contributing factor. Drains were not capable of handling the worst case events and the level of oil water separators across the site were not systematically measured
* The site had a history of spills from pigging activities, including a large fire in 2004, as there were a large number of incoming and outgoing pipelines at the facility. The leak in question occurred in the aftermath of pigging operations

However, the lack of hazard awareness is evident from the fact that a number of personnel had difficulty breathing due to hydrocarbon vapours in the air. Despite this, personnel, some of them fire brigade members, made an effort to start vehicles in order to move around the plant and search for what was clearly a large hydrocarbon leak. The vehicles did not start as the atmosphere was too rich. Eventually the leak, most likely from pigging activities, flowed around the site on the increasingly large volume of water, and found an ignition source.

In another event, in 2009, a large explosion occurred at a CAPECO tank farm in Puerto Rico (Figure 1b). The CSB report (CSB, 2015), outlines the sequence of events, where the offloading of gasoline from a vessel overflowed a storage tank and then ignited, causing a massive explosion and subsequent secondary explosions, damaging 17 of the 48 tanks. There was significant offsite damage to property and the environment, and the fire burned for some 60 hours. Fortunately there were no fatalities. The contributing factors included:

* Malfunctioning level measurement equipment
* Inadequate tank filling procedures and design quirks in the system which meant more than one tank had to be filled at a time, increasing the difficulty in manual fill time calculations
* There were no independent high-high alarm systems or overspill prevention
* Emergency response shortcomings

The lack of hazard awareness is evident in the lack of an appropriate level of caution. When handling an incoming package which is larger than the vessel into which it is being deposited the potential for loss is always high. This is by no means an unusual situation and one wonders how many near misses occurred on this site, which should have acted as warnings. The parallels to Buncefield, which I have not mentioned as the event and investigation is much more well known here in Europe, are obvious.

A person standing in a factory

AI-generated content may be incorrect.A large black smoke billowing from a fire

AI-generated content may be incorrect.

Figure 1a: Reactor layout at Formosa PVC plant (from CSB)

Figure 1b: Fire at CAPECO (from CSB)

The recommendations from the CSB report focused on regulatory shortcomings that allowed many of the contributing factors listed on the previous page to be present. However, both these incidents, neither of which occurred that long ago, show a distinct lack of organisational and personal hazard awareness. This is common in situations where the Process Safety Management (PSM) and Health, Safety and Environment (HSE) functions on a site act as the policeman rather than as a support act to the line management functions. The line management functions are where responsibility for PSM/HSE resides. Within the insurance industry we are typically looking for:

* PSM implemented with element champions at operations or maintenance level
* HSE/PSM function is a facilitator, not the driver
* Auditing is an accepted part of the process
* Leading and lagging Key Performance Indicators (KPIs) are employed to inform management of problem areas and the efficacy of action plans to fix these problems
* One of the elements of the PSM programme focuses on effective operator training, including PSM, to improve hazard awareness and understanding of the safe operating limits within the facility

There are a number of other, less recent, losses with hazard awareness at their heart, including a major oil spill in Michigan in 2010 and a fire at a refinery in California in 1999. Included in the references are the technical reports by the National Transportation Safety Board (NTSB, 2012) and the CSB (CSB, 2001) respectively for these two events, and I'm sure delegates can think of many more.

3.3 Transient Operations

The third type of incident has already been touched on as part of the commentary on the Formosa PVC plant loss. Here I want to briefly digress to refer to the LMA publication referred to earlier. An Analysis of Common Causes of Major Losses in the Onshore Oil, Gas and Petrochemical Industries was published by the Lloyds Market Association in September 2016 and was also presented as a paper at the 2017 Hazards conference. The document contains a detailed review of loss causation in these industries.

Recently there has been work undertaken to update the document to include more recent losses. While this work is not complete at this time, the overall statistical conclusions in terms of loss causation remain largely unchanged.

I recommend the document for a breakdown of the losses into various categories, including across industry types (refining, petrochemicals, other) and, of particular relevance in this topic, across operational status differences. In particular, it is interesting to note that 63% of operational losses (e.g those not related to asset integrity issues) occur during what we call transient operations (Figure 2). These include start-up, shut-down but also emergency situations caused by power or other utility failures and also non-standard operations such as equipment switching. A further 28% occur during maintenance operations.

A pie chart with numbers and text

Description automatically generated

Figure 2: Breakdown of Operational Losses (from LMA)

Many incidents occur during transient operations, and indeed most of the losses above could be used equally well to demonstrate this point. I have turned to some other less known events to further elaborate on the issues raised by transient operations, as it is obvious from the above diagram the part it plays in major losses.

Damage occurred to an oil and gas production platform in offshore Malaysia in 2020. A ship impacted the platform in heavy weather, causing damage to three bridges and the three platforms linked by them, including piping and instrumentation. The ship was anchored only 30m from the platform instead of the 90m required in a heavy swell, which was defined as greater than 2.5m. The sea state at the time was 3.8m. Subsequent damage was less than US$100m, although given previous incidents that have occurred with ship collisions to platforms, notoriously the Mumbai High incident in 2005, this could probably be considered a near miss.

Observations that occur to the author include pending natural hazard events should prompt a review of all relevant procedures and operators should be trained in how to respond to deviations from normal activities, e.g. during abnormal, non-routine or unplanned events.

In 2018 there was a large fire at a petrochemical plant in Saudi Arabia. The fire was caused by overpressure and rupture of a lower pressure (LP) rated blowdown vessel downstream of the high pressure blowdown vessel on the polypropylene (PP) plant. A manual isolation valve in the PP plant blowdown system should be closed at a specific point in the procedure when solids are being drained from the LP vessel, but then reopened afterwards. This did not happen and the system was overpressurised and caused a fire. It became clear during interviews operators were not clear on the procedure and they did not use the checklist except during start-ups and shut-downs. Observations that occur to the author include better use of SCTA would have identified the potential for overpressure and led to a more robust management system around a manual process, and operators should be trained in, and drilled on, the hazards associated with transient operations such as clearing blockages on polymer plants.

There are a number of other, less recent, losses with transient operations at their heart, including a massive vapour cloud explosion (VCE) at a petrochemical plant in Texas and the rather more well known explosion at a gas plant in Australia in 1998. Included in the references are the excellent book by Australian author Andrew Hopkins (Hopkins, 2000) on the latter loss. In fact, for all you need to know about process safety leadership and organisational failures, I would recommend all of the books by the same author.

4. Conclusions

I would like to begin the conclusion by reiterating my first point. The losses I have used as examples all had management failures of one kind or another as their chief cause. These failures are the major cause of these losses, not operator error, which is possibly the most useless phrase ever invented in the field of incident and loss investigation. Attributing a loss to operator error has most likely never helped prevent a similar accident, except for the operators and workers concerned, who now have personal experience as their guide. It would be good if we didn't have to learn lessons this way, though.

Many of these losses occurred during a transient or unusual operation. It is my experience that organisations, even when analysing their processes with tools such as HAZOP, do not adequately address these transient operations. Similarly, the take up of tools such as SCTA, referred to earlier, in industry is poor. However, the focus of this paper is what can we do to improve the response of operators and other workers at the sharp end of incidents. Unfortunately, many organisations use risk analysis tools such as PHA and HAZOP as an excuse to shift the critical actions onto these personnel, rather than relying on design or other engineering (e.g. more costly) solutions.

Also unfortunately, the training of operators and use of drills and simulations frequently does not cover and/or practice the proper response in these transient or emergency states. In the days of higher reliability and greater run lengths between turnarounds, some operators may not experience power interruptions, start-ups or shut-downs for many years. It seems obvious that then expecting operators to behave in a certain way, often in stressful and/or complicated situations, is ambitious at best.

References

Hopkins A., 2000, Lessons from Longford: The Esso Gas Plant Explosion, CCH Australia

Jarvis R. and Goddard A., 2016, An Analysis of Common Causes of Major Losses in the Onshore Oil, Gas and Petrochemical Industries, Lloyds Market Association

Marsh, 2024, 100 Largest Losses in the Hydrocarbon Industry, Marsh

National Transportation Safety Board, 2012, Enbridge Incorporated: Hazardous Liquid Pipeline Rupture and Release, NTSB

Petroleum and Natural Gas Regulatory Board, 2019, Major Fire at ONGC's Gas Processing Plant at Uran, PNGRB

US CSB, 2015, Final Investigation Report: Caribbean Petroleum Tank Terminal Explosion and Multiple Tank Fires, Caribbean Petroleum Corporation, US CSB

US CSB, 2007, Investigation Report: Vinyl Chloride Monomer Explosion, Formosa Plastics Corp., US CSB

US CSB, 2001, Investigation Report: Refinery Fire Incident, Tosco Avon Refinery, US CSB