CHEMICAL ENGINEERING TRANSACTIONS
VOL. 77, 2019
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Genserik Reniers, Bruno Fabiano

ISBN 978-88-95608-74-7; **ISSN** 2283-9216
DOI: 10.3303/CET1977128

Latest Technology to Manage the Complete Process Safety Lifecycle

Enrico Lammers

DWG, Admiraal Lucashof 5, 3115 HM, Schiedam, The Netherlands
enrico.lammers@dwg.nl

Latest developments in software technology allow for the management of the complete Process Safety Lifecycle as defined in standard IEC-61511 for the Process Industry. Most companies in the Process Industry have accepted the necessity of conducting Process Hazard Evaluations e.g. HAZard and OPerability (HAZOP) studies and Layer Of Protection Analysis (LOPA), however it has been more challenging to follow-up on the recommendations and demonstrate that the Safety Instrumented Functions have been built and tested in accordance with the design specifications. Validating the assumptions of the Safety Study and a comparison with actual Process Safety performance in the Plant has proven to be cumbersome and was almost impossible in the past. Furthermore, there was little insight in the financial impact of Process Safety risks. Modern Technology facilitates the validation, hence allowing for the management of the entire Process Safety Lifecycle. Real measured Lead Process Safety KPI's can be produced, controlled and managed.

1. Introduction

The Process Industry has made tremendous progress in reducing Occupational Safety related incidents in the past two decades (Figure 1). Safety statistics are proudly presented in annual reports and on billboards at entrances of Facilities and are implemented in Operational Excellence programs in the majority of the Industry.

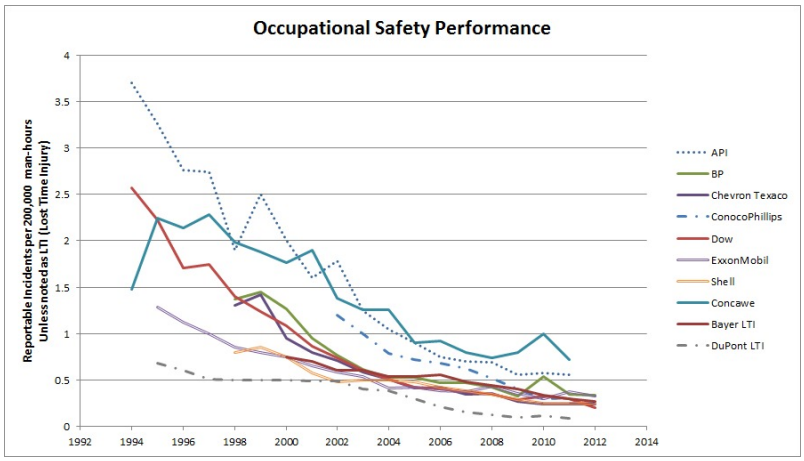

Figure 1: Downward trend on Occupational Safety related incidents (Borges, 2016)

Major, catastrophic incidents on production sites always lead to ex-post investigations by independent agencies and subsequently recommendations are provided to prevent similar incidents in the future. These

Paper Received: 28 November 2018; Revised: 26 April 2019; Accepted: 1 July 2019

Please cite this article as: Lammers E., 2019, Latest Technology to Manage the Complete Process Safety Lifecycle, Chemical Engineering Transactions, 77, 763-768 DOI:10.3303/CET1977128

recommendations typically lead to new Industry Standards, (e.g. IEC-61511 on the Process Safety Lifecycle) revisions, or new Legislation and Directives (e.g. SEVESO on the control of major-accident Hazards involving dangerous substances). Despite these measures, Process Safety related incidents do not show a similar downward trend like Occupational Safety but seem to re-occur over time in a random manner (Figure 2).

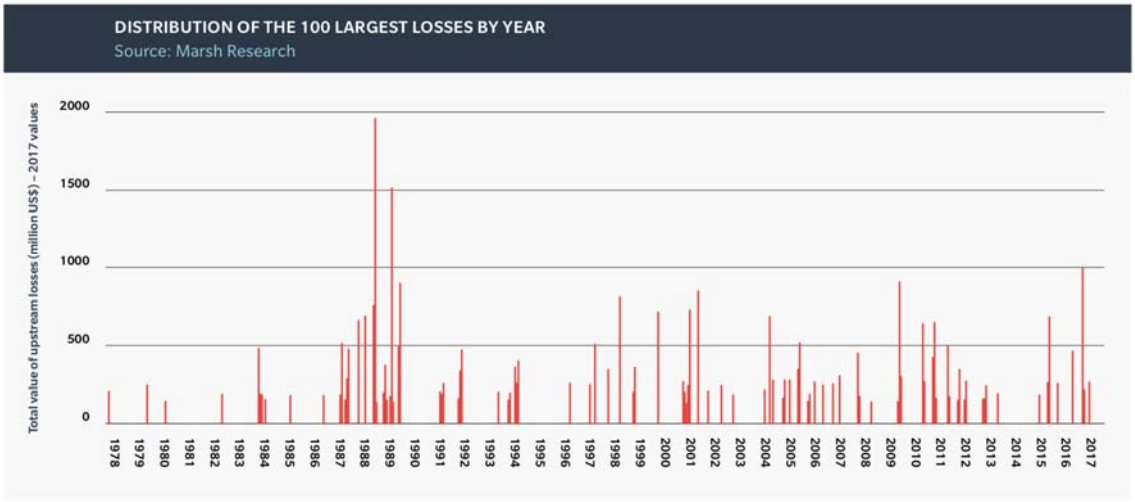

Figure 2: Total value of the 100 largest property losses in Process related Industry in the period 1978-2017 (MARSH, 2018)

The obvious question is: what is the reason for this difference in behaviour between Occupational and Process Safety incidents?

2. Occupational Safety versus Process Safety

Occupational or Personal Safety can be measured directly by visible observations, e.g. does a worker wear protective clothing or hold a handrail? There is a direct connection between the action (hold the handrail) and the benefit (prevention of a fall). Focus on change in behaviour by Safety supervisory programs will lead to improvements in Safety Records and are easily measurable and trackable (e.g. Lost Time Injuries, Lost Work Day Rate, Recordable Injury Frequency etc.).
The playing field of Process Safety is in areas that are not directly visible, e.g. what is the level in the storage tank? What is the critical pressure in that system? Did the operator get the latest design change from the engineer and how do they work together? Process Safety is complicated because it focuses on design, operation and maintenance in order to prevent the loss of system integrity. As Process Safety is not visible, no direct measurements are possible. Only indirect measurements of Safety Records are conceivable which represent only a partial reality.
During an evaluation on the status of Process Safety consciousness in the Industry, 10 years after the explosion at the Buncefield oil storage terminal in Hertfordshire (UK), it appeared that the two key reasons for the relatively low levels of engagement on Process Safety were lack of Leadership and Complacency (processengineering, 2015).

2.1 The role of Leadership in Major Incidents

Many will focus on the specifics of a case such as Buncefield to convince themselves that “it would never happen to me”, while in many boardrooms the reputational and cashflow risks posed by Process Safety incidents are still not fully understood. Excessive focus by senior leaders on Occupational Safety, under the impression that this will control Major Hazards, is misleading or even worse, dangerous. During the Macondo, Deepwater Horizon Rig catastrophe in 2010, the CEO updated the employees of the affected company via an e-mail stating that their safety records were continuously improving, with the Key Metrics such as Recordable Injury Frequency (RIF) and on-site fatalities all showing a downward trend (U.S. Chemical Safety And Hazard Investigation Board, 2016). The Industry persists in treating Occupational Safety and Process Safety statistics in a like manner. (Figure 3a). This suggests that preventing Occupational Incidents also prevents Process Safety Incidents, which appears not to be true. It is more useful to distinguish between the two Safety types

and treat them as mutually exclusive risks (Figure 3b), with their own annual budget, their own implementational and management program and their own responsible manager and accountable senior board member (i.e. Chief Process Safety Officer).

Figure 3: a) Incident pyramid with combined Safety b) Incident pyramids for Personal and Process Safety

2.2 The role of Complacency in Major Incidents

High Reliability Organizations (HRO's) are organisations which are successful in avoiding Major Incidents in an environment where accidents can be expected due to risk factors and hyper complexity (Sutcliffe, 2011). HRO's such as air-traffic control and nuclear powerplants use discomfort and concern about the Management of Risks in a positive way. They use this healthy scepticism to challenge complacency:

- The absence of surprises is regarded as a reason for anxiety, not for complacency
- They are conscious that they might not fully comprehend the complex systems they operate and are preoccupied with failure
- They recognise that Major Hazards are an integral part of their company risk profile and must be managed to that respect.
- They implemented a multi-angled approach of continuous improvement towards Safety issues

Complacency in companies in the Process Industry can be explained by the fact that most of these companies actually have implemented Process Safety Management (PSM) programs on which they manage the risks based on pre-defined Key Performance Indicators (KPI's) or Process Safety Performance Indicators (PSPI's). However, it is the difference in attitude between being continuously critical on the measured KPI's and being satisfied with the outcome of audits on the PSM. It is this attitude which distinguishes HRO's from the vast remainder of the Process Industry. The latter is blinded by the so called "watermelon effect" (ABB, 2017). While the outcome of PSM audits show a healthy performance i.e. green indicator, digging slightly below the surface of the apparent good performance will quickly reveal areas of concern, reflected by the "red flesh". The "watermelon effect" is introduced with the intention to challenge organisations to act like HRO's. This implies being critical to good PSM performance and continuously checking whether the correct amount and type of risk-based metrics are assessed.

2.3 Selection of Key Performance Indicators

In contrast to Occupational Safety, where Safety Records are easily measurable and trackable, the direct and absolute measurement of Process Safety as a whole is not possible due to its complex nature. A combination of Weak Signals might ultimately lead to a large catastrophic event. These weak signals cannot be measured directly but can only be represented by a model i.e. a derivate of the actual situation. Process Safety Performance is measured using specifically defined Performance Indicators, also known as Key Performance Indicators (KPI's). The evaluation of these KPI's must lead to a continuous improvement process. KPI's can either be:

- Leading i.e. actively looking for the holes in the Independent Protection Layers (IPL's). For example: Safety Instrumented Functions (SIF) not tested in time and HAZOP recommendations not closed in time
- Lagging i.e. measured when an event has occurred during normal operation. For example: leakages of equipment or piping

It is key to select the proper type and amount of KPI's, which is not a simple task in practice (Scheepers, 2011)

- Often only a limited number of aspects are measured, so that only a portion of the total performance is evaluated. By focusing on these aspects, there is insufficient attention for other issues.
- There is not always a clear relationship between what is measured and Process Safety. E.g. managing on Occupational Safety metrics will create the false impression that the state of Process

Safety is also good. Even when serious incidents occurred and clearly indicated where the bottlenecks lie, managers continue to believe in the KPI's they measure on

- KPI's are not tailor-made. Many companies use KPI's that are imposed by the parent company or that are common in the Industry. Measuring only these KPI's does not specifically look at the risks of a Company but of the Industry.
- Too few KPI's or unspecific ones are not good, but too many are not good either. This requires too much effort from the Organisation
- Managing the KPI instead of the risk. E.g. the number of closed action points from a Safety Study does not have a direct relation with the quality of the recommendations

3. The role of Modern Technology in Risk Management

In the 3rd Industrial Revolution the automation of production processes occurred, resulting in the development of independent systems. These systems created single data silo's which are used to monitor IPL's (Figure 4a). There is none or only a weak connection between these data systems. In the 4th Industrial Revolution these independent data systems are linked to each other, resulting in a more accurate picture of the real time status of the plant, leading to a Learning Protection Level (LPL) compared to an IPL (Figure 4b) (Petrusich & Volkmar Schwarz, 2017)

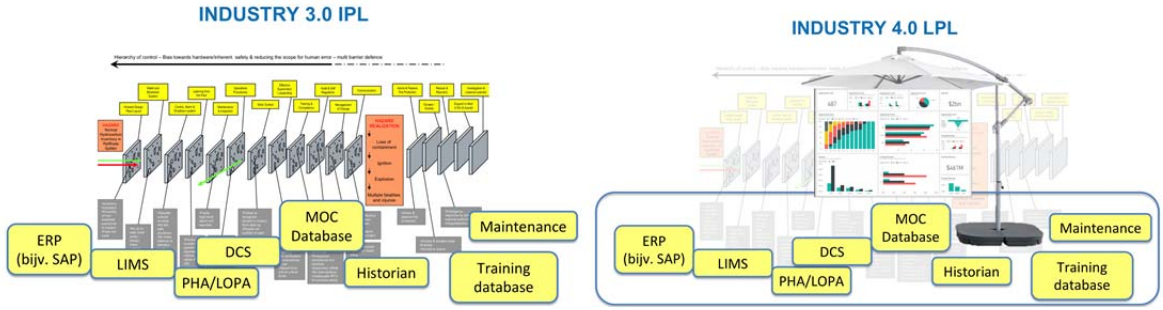

Figure 4: a) Separate data silo's in Industry 3.0 to monitor IPL's b) Interlinked data systems in Industry 4.0

Modern technology facilitates Plant Management in managing KPI's and with that the risk of their plant.

3.1 Process Safety lifecycle as defined in IEC-61511

Industry standard IEC-61511: Functional safety - Safety instrumented systems for the process industry sector, is developed to describe requirements for the engineering and maintaining of Safety Instrumented Systems (SIS), the so-called Process Safety Lifecycle. Typically, the lifecycle comprises three phases: define, monitor and sustain. In the define phase, Compliance documentation, such as a PHA Report (HAZOP), LOPA Report and a Safety Requirement Specification is generated. In the monitoring phase, the accuracy of the assumptions that have been done during the definition phase have to be validated. In the Industry 3.0 era, synchronising massive amounts of reports with operational data has been extremely tedious. In the Industry 4.0 era however, diagnostic interfacing to Maintenance Management systems and Process Historian data systems are easily accessible for this monitoring duty. Monitoring of these systems will reveal relevant Process Safety information like demands on the SIS, aggregate the time in bypass, monitor test intervals and the classification of failures. Monitoring is purposed to clarify whether "bad actors" occur in the Process Safety related systems, in the form of poor assumptions or faulty equipment. A typical way of assessing a risk during a HAZOP and LOPA study is by the use of a Risk Matrix. During the review, a multidisciplinary team assess the Unmitigated Risk (without any form of risk mitigation), the available and required IPL's and the Mitigated Risk. See for example Figure 5. During a HAZOP and LOPA session it was assumed that:

- Effect category C (e.g. a lost time incident or medium leakage or damage between €25k and €100k)
- Frequency[1] for the occurrence of the dangerous scenario (this is the grey circle in the Risk Matrix in Figure 5) is assumed at 1 x per year.
- Credit is taken for an IPL alarm with operator response[2] which reduces the frequency of the dangerous scenario from 1 x per year to 1 x per 10 years
- A SIF[3] is required to reach the acceptable risk area, a further reduction from 1 x per 10 years to 1 x per 1000 years

Figure 5: Risk and Risk Reduction assumptions in HAZOP and LOPA studies

However, in reality during normal operation:

- Incident investigations at the facility have shown that the occurrence of the dangerous scenario is 5 x per year instead of 1 x per year. This moves the starting point on the risk matrix to the right.
- The maintenance history shows that the alarm has been tested regularly and the operator has been trained properly. The credit taken for the alarm has been validated in the HAZOP (actual risk reduction by the alarm is equal to the assumption).
- The maintenance history shows that the components in the SIF were tested much later than the test interval defined in the Safety Requirement Specification (SRS). This leads to a degradation of the SIF to 75% of the design (actual risk reduction by the SIF is smaller than in the assumption).

These three added up, leads to a gap between the assumed and actual risk (Figure 6) and can be visualised on a dashboard (Schuler & Scott, 2017). It is an evergreen leading Process Safety KPI, which gives insight in the current Risk State of the plant. A value less than 100% indicates an under-protection, a value higher than 100% indicates an over-protection and a value of 100% indicates that the assumed and acceptable risk of the company match exactly.

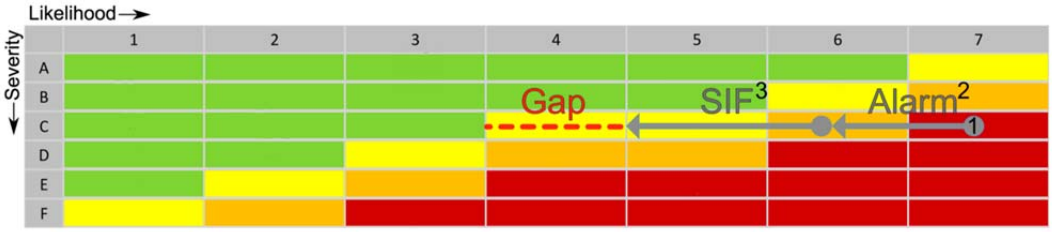

Figure 6: Actual risk and risk reduction during normal plant operation

As bad actors increase the likelihood of a Loss of Primary Containment (LOPC) event, the next phase in the Process Safety Lifecycle is the sustain phase. The sustain phase is meant to maintain the SIS integrity and to manage changes during the life-time. The aim is to remove bad actors which are identified through monitoring in order to remove the risk from the business. In addition, the bad actor may prove to be performing in an overly conservative manner. Therefore, scarce resources which are focusing on over-protected scenarios can be re-aligned to address gaps in underperforming scenarios.

3.2 Financial Risk Profile in relation to Process Safety

The gap which can be visualised by the interrelated data platform of Industry 4.0 not only represents the safety state of the company, but can be used to show the Financial Risk profile as well.
The majority of Companies in the Process Industry are insured for direct financial damage, but usually not for the consequences such as loss of production, consequential damages and third-party claims. An international insurance company has investigated that the gap between economic damage and insured damage is increasing. In 2015, the size of that gap was $ 55 billion. The uninsured losses in the past 10 years have more than doubled compared to the previous 10 years. (Suchak, 2016). Each cell in the Companies Risk Matrix not only represents safety and environmental consequences, but also financial impact. Giving insight in the gap between acceptable and actual financial Risk will assist the Companies in allocating the right expenditures in investments in Process Safety and might lead to lower insurance fees.

4. Conclusions

Due to lack of Leadership and Complacency, Process Safety related incidents in the Industry still occur randomly and do not show the same downward trend as does Occupational Safety. This is related to the persistent belief that Key Metrics for Occupational Safety can be used to monitor and manage Process Safety performance as well. Which is not true. Both types of Safety should be treated independently. The choice of the right type and amount of Key Performance Indicators is essential in Risk Management. The non-related data silo's in the past made integration of Process Safety Information tedious. Modern technology allows for interaction of several data sources and facilitates real-time monitoring of Risks in the plant. This will give better insight in Process Safety and Financial risks of the Company. With the addition of a Chief Process Safety Officer on the board of Industrial Companies, management of Major Hazards can be improved and sound decisions on Process Safety related investments can be made.

References

ABB. (2017). *Avoiding the 'watermelon' effect. Are we doing enough in the process industry to prevent the next major accident?* Retrieved from <www.abb.com/cawp/seitp202/0cf0cbd04a17915cc12581450045a124.aspx>

Borges, V. (2016, January 8). *Perfect storm for the next major accident?* Retrieved from <www.dnvgl.com: blogs.dnvgl.com/software/2016/01/perfect-storm-for-the-next-major-accident/>

MARSH. (2018). *The 100 Largest Losses 1978-2017, Large Property Damage Losses in the Hydrocarbon Industry 25th edition.* MARSH.

Petrusich, J., & Volkmar Schwarz, H. (2017). Industry 4.0 for Process Safety Handbook. Columbia, SC, United States: ISBN: 978-1979021166.

processengineering. (2015, 03 11). *Safety: a ticking timebomb*. Retrieved from <processengineering.co.uk/article/2020018/a-ticking-timebomb>

Scheepers, J. (2011). *Prestatie-indicatoren voor procesveiligheid.* Delft: Delft Toptech.

Schuler, T., & Scott, M. (2017, January 15). *aeSolutions-Justifying-IEC61511-Spend.* Retrieved from <www.aesolns.com/whitepapers/justifying-iec-61511-spend/aesolutions-justifying-iec61511-spend/>

Suchak, S. (2016). *Red alert: The hidden safety risks companies aren't disclosing.* Schroders.

Sutcliffe, K. M. (2011, July 27). High reliability organizations (HROs). *Best Practice & Research Clinical Anaesthesiology*, 133-144. Retrieved from Wikipedia: <en.wikipedia.org/wiki/High_reliability_organization>

U.S. Chemical Safety And Hazard Investigation Board. (2016). *Drilling Rig Explosion and Fire at the Macondo Well.* U.S. Chemical Safety And Hazard Investigation Board.