MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

19th Annual International Symposium
October 25-27, 2016 • College Station, Texas

Process Safety-Equations of State

Brian R. Dickson,
Dept. Chemical & Process Engineering
University of Strathclyde, Glasgow, G1 1XJ, UK.
Email: brian.dickson@strath.ac.uk

Abstract

By convention, chemical engineering requires us to develop a set of empirical equations that predict the transformation of one state into another. Process Safety generally lacks that discipline and as a consequence is sometimes suggested as having a lack of academic rigour. (Apologies here to the hard working risk, fires & explosions modellers)

In the tradition of empirical chemical engineering, this paper takes a philosophical approach to "equations of state" as a way of demonstrating the transitions that have taken place in the approaches to Process Safety, consider the rise and fall of the importance of key components and present a "hypothesis" for discussion, that there is a "need to move away from the Engineering model and its linear solutions, to an Organizational Model where responsibility lies with the Individual rather than the System which is still the current trend." [1]

In reviewing this text, readers are provided with excerpts from an Events History of Process Failure which is intended to be indicative rather than prescriptive in its nature. It is taken from a wide arrange of sources only to demonstrate the frequency of major events across large parts of the world-wide process industry.

Key Words: Process Safety Management, Risk, Human factors,

Introduction

In the mid 70's, two non-connected events occurred, the author completed his BSc in Chemical Engineering and in the UK, the "Health & Safety at Work" Act came into place. The latter, largely unchanged in concept today, gave us ALARP and made the author possibly legally responsible for actions likely to cause death or injury to employees, contractors and members of the public by his actions as a professional chemical engineer or so may line-manager said. My employer gave me a training course on the Act and its implications and reminded me that responsibility lies in my actions as a professional chemical engineer. On reflection, none of that presumption of responsibility was misplaced or changed, yet to date no individual in the process sector in the UK has been prosecuted, even though a substantial number of companies have met that fate.

Events logged included:

Date	**Event Name**
1974	Flixborough
1976	Seveso
1979	3 Mile Island

Table 1: Events having potential to change Process Safety Practice 1970-1999

So my First Equation of State is based upon practice as a chemical engineer, who had never had a class in process safety, and is suggested as;

Safety Practice (SP) =
F (Materials of Construction (M_c), Property of Materials (P_m), Reaction Kinetics (R_k), Effect of Fires & Explosions (E_{fe})),

written as; $$SP= F [M_{c,} P_{m,} R_{k,} E_{fe}] \quad (1)$$

and my source of reference: Perry.

By the 80's, things were getting a lot more serious, Safety Teaching in Under-graduate courses is now common place

Events logged included:

Date	**Event Name**
1984	Bhopal,
	Mexico City
1986	Chernobyl
1998	Piper Alpha
1989	Phillips Pasadena

Table 2: Events having potential to change Process Safety Practice 1980-1989

and equation 1 had to be modified to include: HAZOP (H_z), LOPA (L_{pa})

and became Second Equation of State written as; $SP = F [M_c, P_m, R_k, E_{fe}, H_z, L_{pa}]$ (2)

and my source of reference: Perry, Lees.

From the 90's, industry performance remains constant and Texas A & M and University of Sheffield move teaching to a Post- graduate level course and it was imbedded in University of Strathclyde full and part time Masters courses. The latter results in around 8% of degree credits having a process safety content.

Events logged included:

Date	Event Name
1990	Arco, Texas
1994	WNC-Nitro Chemicals, Germany
1995	Albright & Wilson, Oldbury, UK
1998	Longford, Australia

Table 3: Events having potential to change Process Safety Practice 1990-1999

Equation 2 had to be modified to include: Safety Case/COMAH (S_c), QRA(Q_{ra}),

and became Third Equation of State written as; $SP = F [M_c, P_m, R_k, E_{fe}, H_z, L_{pa}, S_c, Q_{ra},]$ (3)

and my source of reference: Perry, Lees, CCPS (Eng. Design for Process Safety) Kletz (What went wrong)

When we reach the 2000 decade, Management of Safety becomes a real driving force and equation 3 had to be modified to include: Management of Change (M_{ch}), Swiss Cheese Model (S_{cm}) and Safety Management Systems (SMS)

and became Fourth Equation of State written as;

$$SP = F [M_c, P_m, R_k, E_{fe}, H_z, L_{pa}, S_c, Q_{ra}, M_{ch}, S_{cm}, SMS] \quad (4)$$

Events logged included:

Date	Event Name
2001	Conoco Humber AZF Toulouse
2004	Skikda LNG Algeria
2005	Texas City Mumbia High North Field Buncefield Songhua River, China
2009	Caribbean Pet Corp Tank Farm

Table 4: Events having potential to change Process Safety Practice 2000-2099

and my source of reference: Perry, Lees, CCPS (Eng. Design for Process Safety) Kletz (What went wrong), IChemE (Hazop), Reason (Human Factors), CCPS (Implementing Process Safety Management System)

Finally, arriving at the 2010's decade which is still underway, we are presented by a worrying trend of failures in large companies who have bon-fide safety systems in place yet are suffering from a breakdown in procedure. Safety case has changed by virtue of COMAH becoming COMAH2 (C_h^2)
Events logged included:

Date	Event Name
2010	Deep Water Horizon/Mocondo Dupont Belle Tesoro Refinery
2012	US Ink Chevron Richmond, CA
2013	Williams Olefins
2014	Du Ponte Porte
2015	ExxonMobil Torrance, CA
2015	Tianjin, China

Table 5: Events having potential to change Process Safety Practice 2010-2016

and equation 4 had to be modified to include: Leading/Lagging Indicators (L_{li}), Stress Cracking (S_{cr}), Management of Safety Competence (M_{sc})
and became Fifth Equation of State written as;

$$SP= F [M_{c,} P_{m,} R_{k,} E_{fe,} H_{z,} L_{pa,} S_{c,} Q_{ra,} M_{ch,} S_{cm,} Ch^2, Lli, S_{cr,} M_{sc}] \quad (5)$$

and my source of reference: Perry, Lees, CCPS (Eng. Design for Process Safety) Kletz (What went wrong), IChemE (Hazop), Reason (Human Factors), CCPS (Implementing Process Safety Management System), CCPS (Integrating Management Systems & Metrics to improve Process Safety Performance) and 30 other books on my shelf **but lastly Dekker [2] (Drift into Failure)**

and was perhaps now impossible to solve. **Or was there a link in M_{sc} and Drift into Failure**

Discussion

At this point, we need to ask why nothing appears to have change, events still occur although some writers suggest that performance is improving because we are killing less people as more have become employed.

To understand why there is still a problem, it's worth considering some of the writing son the causes of this Atrophy of Progress and the lessons that need to be drawn.

Charles Perrow [3], an organizational theorist, suggests a bleak proposition that "accidents are inevitable in complex, tightly-coupled systems ……...regardless of the skills of their operators and managers."

Hence the title: accidents in such systems are 'normal'" According to Perrow the redundancies that go to make up defences-in-depth have three dangerous features.

1. Redundant defensive back-ups increase the interactive complexity of high-technology organizations and thus increase the likelihood of unforeseeable common-mode failures. While the assumption of independence may be appropriate for purely technical breakdowns, human errors at the 'sharp end', in the maintenance sector and in the managerial domains are uniquely capable of creating failures that can affect a number of defensive layers simultaneously"
2. Adding redundancy makes the system more opaque to the people who nominally control and manage it. Undiscovered errors and other latent problems accumulate over time and increase the likelihood of the 'holes' in the defensive lining up to permit the passage of an accident trajectory. This alignment of the gaps can be created either by interactive common-mode failures or by the simultaneous disabling of supposedly independent defences, as at Chernobyl.
3. As a consequence of this dangerous concealment, and because their obvious engineering sophistication, redundant defences can cause systems operators and managers to forget to be afraid. This false sense of security prompts them to strive even higher levels of production. Fixes including safety devices, often merely allow those in charge to run the system faster, or… with bigger explosives"

Karl Weick reinforces this view of unstable systems in control and tells us that "We know that single causes are rare, but we don't know how small events can become chained together so that they result in a disastrous outcome. In the absence of this understanding, people must wait until some crisis actually occurs before they can diagnose a problem, rather than be in a position to detect a potential problem before it emerges.

To anticipate and forestall disasters is to understand regularities in the ways small events can combine to have disproportionately large effects." [4]

In taking forward this view, we appear to set ourselves a challenge of inevitable failure and if one were to take a pessimistic view of the safety history of the process industries then this may well be the case. Although this is where Reason[5] brings us and this papers challenge in "Making Sense of Reason". His "Safety Space" is a natural extension of the resistance-vulnerability continuum introduced in the previous section. It is a boundary within which the current resistance or vulnerability of an individual or an organization is represented. As shown in Figure 1, it is cigar-shaped, with extreme resistance located at the left-hand end and extreme vulnerability at the right-hand end. The shape acknowledges that most people or organizations will occupy some intermediate point within this space.

An organization's position within the safety space is determined by the quality of the processes used to combat its operational hazards. In other words, its location on the resistance-vulnerability dimension will be a function of the extent and integrity of its defences at anyone point in time. However, here is no such thing as absolute safety, human fallibility, latent conditions and the possibility of chance conjunctions of these accident-producing factors continue to exist, even the most intrinsically resistant organizations-those at the extreme left-hand end- can still have

accidents. By the same token, 'lucky' but unsafe organizations at the extreme right-hand end of the space can still escape accidents for quite long periods of time.

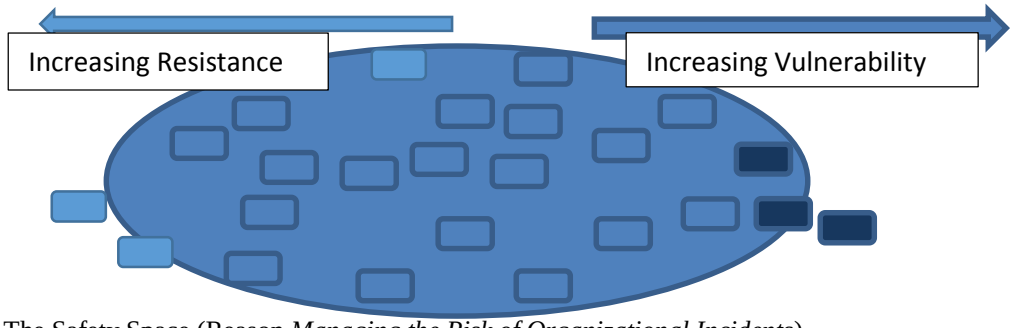


Fig 1: The Safety Space (Reason *Managing the Risk of Organizational Incidents*)

"The key to navigating the safety space lies in appreciating what is manageable and what is not. Many organizations treat safety management as a negative production process, they set reduced negative outcome targets for the coming accounting period (e.g., 'Next year we'll reduce our lost-time accidents by half'), yet accidents by their nature, are not directly controllable, so much of their causal variance lies outside the organization's sphere of influence. The organisation can only defend against hazards; it cannot remove or avoid them and still stay in business. Similarly, an organization can only strive to minimize unsafe acts, it cannot eliminate them altogether, and figure 2 demonstrates some of the high level factors that need to be in place."

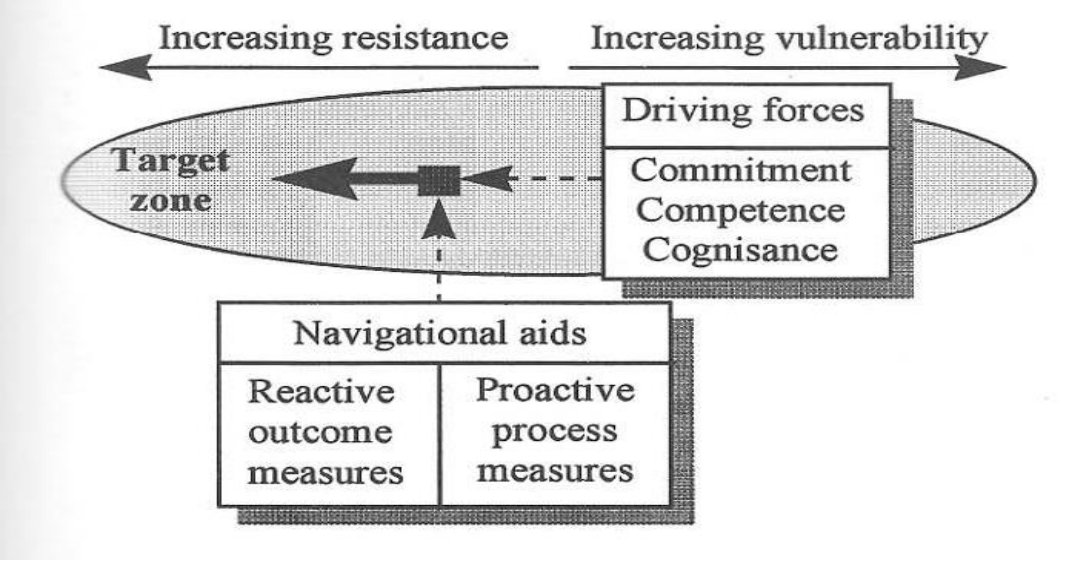


Fig 2: A summary of the principal factors involved in navigating the "Safety Space" with The Driving Forces and the Navigational Aids that together comprise the safety information system (Reason *Managing the Risk of Organizational Incidents*)

Conclusion

Effective safety management is more like a long-term fitness programme than negative production. Rather than struggling vainly to exercise direct control over incidents and accidents, managers should regularly measure and improve those processes--design, hardware, training,

procedures, maintenance, planning, budgeting, communication, goal conflicts, and the like-that are known to be implicated in the occurrence of organizational accidents. These are the manageable processes determining a system's safety health. They are, in any case, the processes that managers are hired to manage; safety management is not an add-on, but an essential part of the system's core business.

Perhaps safety indictors need brought into the management world, where there is no room for "loss time statistics", "leading/lagging indicators", or current position on the "Heinrich's Safety Triangle/Dashboard" and more about:

- Did the work force feel safe at work today?
- What did we do safely today to make the business more secure?
- What marginal gains have we developed today to make us all safer?

These are perhaps 3 from many indicators to be used by managers who normally show concern about the viability of their business by asking about Quality (throughput) & Financial (Cash at bank) indicators.

However, there is a challenge in this view and in addressing "why", it's is suggested here that the concept of competence or the lack of it is the problem.

In his review of "Texas City Refinery Explosion: Lessons Learned", Mogford [6] mentions five underlying causes, all management responsibilities and two in particular are linked to the theme of this paper:

> "Secondly, process safety, operations performance and systematic risk reduction priorities had not been set nor consistently reinforced by management. Safety lessons from other parts of BP were not acted on.
>
> And finally, poor performance management and vertical communication in the refinery meant there was no adequate early warning system of problems and no independent means of understanding the deteriorating standards in the plant through thorough audit of the organisation."

This is reinforced in the Baker [7] commission report for BP,

> **"Recommendation #3**
> **– process safety knowledge and expertise**
> BP should develop and implement a system to ensure that its executive management, its refining line management above the refinery level, and all U.S. refining personnel, including managers, supervisors, workers, and contractors, possess an appropriate level of process safety knowledge and expertise."

BP and many other companies have done much in progressing this idea, yet CCPS's *Guidelines for Auditing Process Safety Management Systems* (2nd edition 2011) places "Training and Performance Assurance" at p547 out of 835, and this really returns to the start of this paper, if the senior management don't understand

The Process Safety First Equation of State;

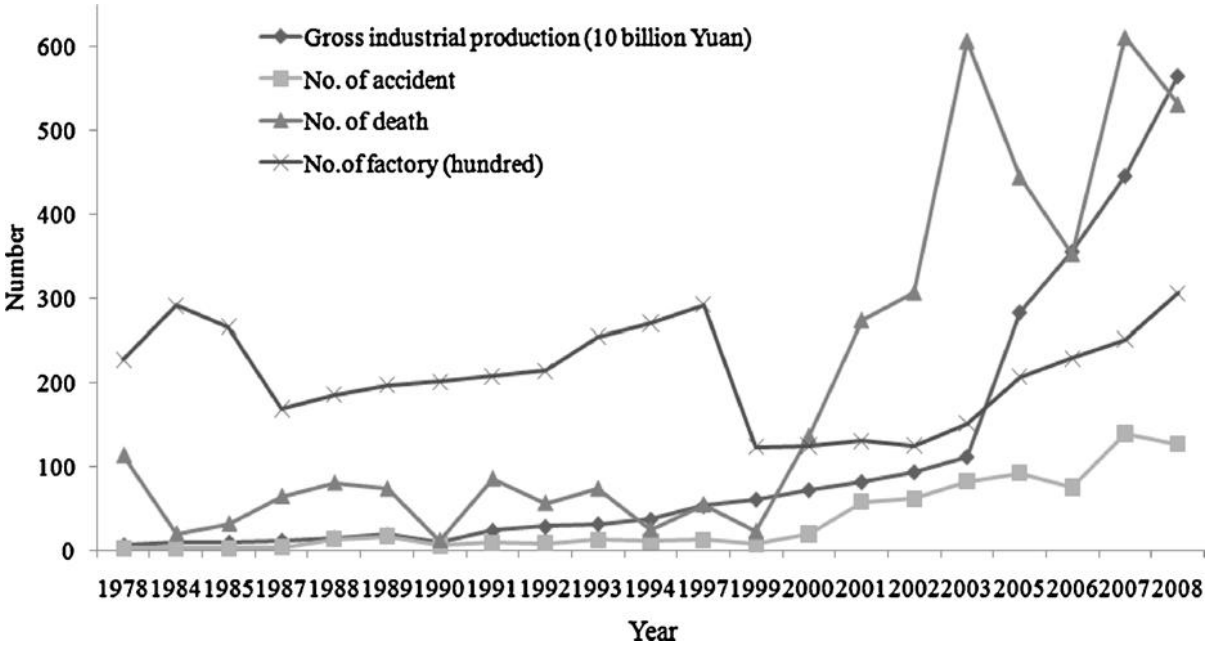
Safety Practice (SP) =
F (Materials of Construction (M_c), Property of Materials (P_m), Reaction Kinetics (R_k), Effect of Fires & Explosions (E_{fe})),

Just understanding Cash Flow, Six Sigma, Coaching & Leadership and all the other chapters of *"How to be an Even Better Manager: A Complete A-Z of Proven Techniques and Essential Skills"* or some other book of that ilk, is not being a manager and the anthology of Process safety events presented in this paper will continue.

As a closing statement, I met recently with a senior executive who had just return from a court case where his company pled guilty to causing the death of one of its workforce. He hadn't been around during the time of the event, yet was deeply affected by the pain still being suffered by the victims' relatives. Needless to say, his actions in involving his directors and line managers in managing safety are changing radically.

Further Reading

In closing this paper and in support of the argument presented, I would urge readers to consider G. He, L. Zang, Y. Lu & A. Mol: "Managing major Chemical accidents in China: Towards effective risk information" Journal of Hazardous Materials March 2011 for the statistics presented and in particular one which is reproduced below and follow the line "no. of deaths".



References

[1] Dickson B.R: Making Sense of Reason: A review of the message James Reason put forward for a re-think of Safety Management Principles, AIChE,11th Global Congress on Process Safety Proceedings, 2015

[2] Dekker Sidney: Drift into Failure Ashgate Publishing 2011

[3] Perrow Charles: Normal Accidents: Living with High risk Technologies, Basic Books, 1984

[4] Weick Karl quoted in P.J. Frost et al.: Reframing Organizations Sage 1991

[5] Reason James: Managing the Risk of Organizational Incidents, Ashgate Publishing, 1997

[6] Mogford J: The Texas City Refinery Explosion: The Lessons Learned**,** AIChE,2nd Global Congress on Process Safety Proceedings, 2006

[7] Baker J: BP US Refineries Independent Safety Review Panel Report, 2007