# Managing Process Safety

Core Body of Knowledge for the Generalist OHS Professional

Third Edition, 2024

13

AIHS

Australian OHS Education Accreditation Board

## Copyright notice and licence terms



## Disclaimer

# Acknowledgements



The Australian Institute of Health & Safety (AIHS) financially and materially supports the *OHS Body of Knowledge* as a key requirement of the profession.

The *OHS Body of Knowledge* forms the basis of the AIHS OHS capability agenda and informs the other platforms of the agenda: education assurance through accreditation; role clarity, capability assurance through individual certification and continuing professional development.

Thus, the *OHS Body of Knowledge* is strategically important to the AIHS and vital for the profession. (www.aihs.org.au).


The *OHS Body of Knowledge* provides a framework for OHS professional education and continuing professional development. As the body managing accreditation of OHS professional education, the Australian OHS Education Accreditation Board influences, supports and monitors the *OHS Body of Knowledge*, and has a major role in the development and review of individual chapters to ensure that the quality and evidence base reflects current OHS research and leading-edge thinking, and so provides a suitable standard for OHS education and professional development.
www.ohseducationaccreditation.org.au


The IChemE Safety Centre (ISC) is a not-for-profit industry-led organisation with a vision to be a global go to organisation for process safety benchmarking, sharing of best practice and education, and be a forum for developing solutions to common problems. This collaboration with the OHS Body of Knowledge fits with ISC strategic direction to maintain close connections with other like-minded organisations and set the benchmark for process safety across industry and academia.

## Bibliography

ISBN 978-0-9808743-3-4

## First published in 2017

### Authors

Trish Kerin, Director, IChemE Safety Centre, Institution of Chemical Engineers

Peer reviewers

| | |
|---|---|
| Sidney Abiodun | Senior Inspector Onshore, Major Hazards Facility, WA Department of Mines and Petroleum |
| Kym Bills | Executive Director, National Resource Sciences Precinct, Perth |
| Simon Farrar | Manager Systems Safety, WorkSafe Victoria |
| Jan Hayes | Associate Professor, RMIT University |
| Peter Hicks | Prelude Production HSSE Manager, Shell Australia |
| Andrew Hopkins | Emeritus Professor, Australian National University |
| Jennifer Lourie | Production AIPSM Lead, Shell Australia |
| Vince McNeilly | General Manager, McNeilly Consulting, UK |
| Tony Pooley | CEO, Principle Seven |
| Leo Ruschena | Senior Lecturer, RMIT University |
| David Skegg | Lecturer, Central Queensland University |
| Derek Viner | Associate Professor, Central Queensland University |
| Laurentiu Zamfirescu | Senior Inspector (Technical Process Safety), WA Department of Mines and Petroleum |

## Third Edition published in 2025

Chapter re-published with updated references and minor content update.

### Author

Trish Kerin, Director, Lead Like Kerin

Citation of the whole *OHS Body of Knowledge* should be as:

> AIHS (Australian Institute of Health & Safety). (2024). *The Core Body of Knowledge for Generalist OHS Professionals*. 3rd Ed. Kensington, VIC: Australian Institute of Health and Safety.

Citation of this chapter should be as:

> Kerin, T. (2025). Managing Process Safety. In *The Core Body of Knowledge for Generalist OHS Professionals*. 3rd Ed. Kensington, VIC: Australian Institute of Health & Safety.

# Managing Process Safety

**Trish Kerin** BEng(Mech)(Hons), DipOHS, MLdrshp, GAICD, CEng, FIChemE, Professional Process Safety Engineer, FIEAust, Senior Member AIChE

Director, Lead Like Kerin

Email: trish@leadlikekerin.co.

Trish Kerin is an award-winning international expert and key note speaker on process safety leadership and was the inaugural director of the IChemE Safety Centre. She helps organisations share and learn in process safety. Trish leverages off her years of engineering and varied leadership experience to help organisations improve their process safety outcomes.

She has represented industry on many government committees and has sat on the board of the Australian National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA). She previously sat on the Mary Kay O'Connor Process Safety Center (MKOPSC) steering committee at Texas A&M University and is the Chair of the WorkSafe Victoria Major Hazards Advisory Committee.

She is a Chartered Engineer, registered Professional Process Safety Engineer, Fellow of IChemE and Engineers Australia and a Senior Member of AIChE. Trish holds a Diploma in OHS, a Master of Leadership and is a Graduate of the Australian Institute of Company Directors.
Her expertise has been recognised with the John A Brodie Medal (2015), the Trevor Kletz Merit Award (2018) and Women in Safety Network's Inaugural Leader of the Year (2022). She has been named one of the "Superstars of STEM" for 2023/24 by Science and Technology Australia.

# Topic Specific Technical Panel

Members of the Topic Specific Technical Panel (2nd Edition) and authors were selected on the basis of their demonstrated specialist expertise. Panel members were not remunerated; they provided input and critical comment as part of their contributions to the OHS profession and to workplace health and safety.

| | | |
|---|---|---|
| Trish Kerin | Chair | Director, Lead Like Kerin |
| Pam Pryor | OHSBOKEA liaison | Registrar, Australian OHS Education Accreditation Board |
| Joe Aiken | Topic specialist | Consultant, Safety Solutions |
| Andrew Battye | Topic specialist | Team Coordinator, Dangerous Goods & Explosives, SafeWork NSW |
| Daniel Grivicic | Topic specialist | Lead Engineer, Machine Safety, Electro80 |
| Roisin Johnson | Topic specialist | Manager, Risk Engineering, WorleyParsons |
| Yogesh Koirala | Topic specialist | Researcher, Mary Kay O'Connor Process Safety Center, Texas |
| Fiona Murfitt | Generalist OHS professional | Group HSSE Manager, Viva Energy |
| Ivica Ninic | Topic specialist | Principal Process Safety Engineer, Origin |
| Alan Munn | Topic specialist | Consultant, MMI Engineering |
| Chad Pettitt | Generalist OHS professional | Lead Consultant, AusSafe |
| Zeeshan Qureshi | Topic specialist | Inspector, Major Hazards Unit, SafeWork NSW |
| Vanessa Russell | Generalist OHS professional | Principal Advisor HSE, Origin |
| Tony Smith | Generalist OHS professional | Manager, Business Risk, East Gippsland Water |
| Jon Temby | Generalist OHS professional | Director, Axento Safety |
| Andrew Woodhams | Topic specialist | Director, Safety Programs, Australian Petroleum Production & Exploration Association |

## Core Body of Knowledge for the Generalist OHS Professional

# Managing Process Safety


## Abstract

Process safety incidents have resulted in thousands of deaths, severe environmental damage, and massive property and business losses. Process safety is usually seen as the responsibility of process safety or chemical safety experts. However, limiting the management of process safety to process safety professionals ignores the contribution of generalist occupational health and safety (OHS) professionals and the value of an integrated, collaborative approach. As a companion chapter to *OHS Body of Knowledge* Chapter 17.4 Process Hazards (Chemical), this chapter provides information vital for the effective engagement of generalist OHS professionals in the management of process safety. After defining process safety, the chapter provides contextual information from historical and legislative perspectives, and considers the impact of process safety incidents on people, the environment and businesses. The core of the chapter focuses on clarifying the roles of process safety professionals and generalist OHS professionals, and reviewing process safety-related hazard identification, risk assessment and control from an OHS perspective. Finally, implications for OHS practice are discussed. As an impetus for change to both process safety and OHS practice, this chapter should facilitate improved safety in all process and hazardous chemical environments.



## Keywords

process safety, failure, control, competencies


### Contextual reading

Readers should refer to 1.2 Contents for a full list of chapters and authors and 1.3 Synopsis of the OHS Body of Knowledge. Chapter 2, *Introduction* describes the background and development process while Chapter 3, *The OHS Professional* provides a context by describing the role and professional environment.

### Terminology

Depending on the jurisdiction and the organisation, Australian terminology refers to 'Occupational Health and Safety' (OHS), 'Occupational Safety and Health (OSH) or 'Work Health and Safety' (WHS). In line with international practice this publication uses OHS with the exception of specific reference to the Work Health and Safety (WHS) Act and related legislation.

### Jurisdictional application

This chapter includes some reference to Australian safety legislation. This is in line with the Australian national application of the *OHS Body of Knowledge*. Readers working in other legal jurisdictions should consider these references as examples and refer to the relevant legislation in their jurisdiction of operation.

# Table of contents

## List of Figures



## List of Tables

# 1 Introduction

Process hazards, and failures in the management of them, have caused disasters resulting in thousands of deaths, severe environmental damage, and property and business losses amounting to billions of dollars. Historically, process safety has been managed separately to occupational health and safety (OHS). However, a factor common to many process safety incidents has been a failure by management to distinguish between process safety and personal or occupational health and safety.[1]

While the distinction between process safety and OHS is important, there are similarities and overlap between the two fields of expertise and a need for collaboration. This chapter and the *OHS Body of Knowledge* companion chapter, 17.4 Process Hazards (Chemical), aim to identify process safety-specific information that underpins the management of process hazards and to make it accessible to generalist OHS professionals. Such knowledge will enable them to operate successfully in process and high hazard environments and engage effectively with process safety professionals.[2] An understanding of the principles of managing process hazards will enhance the practice of all OHS professionals, not just those working in a process safety environment. While some generalist OHS professionals will have an engineering background, the chapter content does not make this assumption.

The primary target audience for this chapter includes generalist OHS professionals:

- Working in major hazard facilities or other process environments with process safety professionals or
- Working in facilities with process safety issues where process safety professionals are not available on site but may be available on a consulting basis or
- Seeking an understanding of process safety concepts to inform their practice more generally.

Secondary target audiences include process safety professionals seeking understanding of the role and knowledge base of the generalist OHS professional to facilitate communication and collaboration across the two professional groups, and non-technical people working in process safety environments who will benefit from some understanding of the principles of process safety.

[1] See, for example, *Lessons from Longford: The Esso Gas Plant Explosion* (Hopkins, 2000) and *Failure to Learn: The BP Texas City Refinery Disaster* (Hopkins, 2008).

[2] For the purposes of this chapter the term ‘process safety professional’ includes process safety engineers and others who may be considered process safety specialists.

This chapter and the companion chapter, Process Hazards (Chemical), support achievement of the *Australian Work Health and Safety Strategy 2023-33* vision for "safe and healthy work for all" (SWA, 2023a, p. 4). This strategic objective is to be achieved by reducing exposure to hazards and risk with improved controls. A broad understanding of the principles of process safety will contribute to better hazard controls as well as to reduced risk of a catastrophic event. These chapters underpin the strategic outcome that "Education, innovation, and collaboration will be critical enablers of our success." (SWA, 2023, p. 5).

After defining process safety, the chapter provides contextual information from a historical perspective and considers the impact of process safety incidents on people, the environment and businesses. A brief overview of approaches to relevant legislation is followed by clarification of the roles of the process safety professional and the generalist OHS professional in process safety, and hazard identification, risk assessment and risk control are considered from an OHS perspective. Finally, implications for OHS practice are discussed. Appendix 1 provides a list of acronyms used by process safety professionals that may be useful for the generalist OHS professional.

Discussions undertaken as part of chapter development demonstrated that a clear understanding by all stakeholders of the respective roles of the process safety professional and the generalist OHS professional will benefit process safety and collaboration among those involved.

## 1.1 Process for developing the chapter content

The initial chapter was the outcome of a joint project of the Institution of Chemical Engineers (IChemE) Safety Centre (ISC) and the Safety Institute of Australia (SIA) (now AIHS). The chapter scope and content was determined by a technical panel of process safety professionals and generalist OHS professionals. In some cases, members of the technical panel also contributed text. A chapter draft was reviewed by a number of process safety and generalist OHS professionals with the final version being the result of professional editing to ensure consistency with other chapters of the *OHS Body of Knowledge*.

In 2024 the author reviewed the chapter for the 3rd edition to ensure the content remains relevant and up-to-date. The following minor changes were made:

- The addition of recent process safety incidents.
- Identification of different global approachs.
- Update to categories of ISD.
- Movement of sections to improve flow.
- Updated references.

## 1.2 Definition of process safety

It is generally accepted that 'process safety' is about preventing incidents that, while having a low likelihood of occurrence, are associated with severe potential consequences. However, one of the challenges in writing this chapter stemmed from the lack of an accepted definition. In practice, discussions of process safety often refer to 'major hazards', which brings in the concept of major hazard facilities (MHFs) such as oil refineries, chemical plants, mines and other sites where large quantities of hazardous materials are stored, handled or processed, and have historically been the source of major incidents. In many countries such sites come under specific legislation with detailed safety management requirements imposed on the site operators. While the content of this chapter will be useful to those generalist OHS professionals working in MHFs, it takes a much broader view of process safety.[3]

One commonly cited definition of process safety is published by the American Institute of Chemical Engineers' (AIChE) Center for Chemical Process Safety (CCPS).[4] However, the technical panel advising the development of this chapter considered that the CCPS definition warranted amendment with greater emphasis on potential loss of control rather than potential loss of containment. This subtle difference in focus can be the key to prevention of incidents and minimisation of consequences.

Hence this chapter applies the following definition of process safety that draws on, but amends, the CCPS definition:

> *Process safety* is about managing the integrity of operating systems by applying inherently safer design principles, engineering and disciplined operating practices. It deals with the prevention and mitigation of incidents that have the potential for a loss of control of a hazardous material or energy. Such loss of control may lead to severe consequences with fire, explosion and/or toxic effects, and may ultimately result in loss of life, serious injury, extensive property damage, environmental impact and lost production with associated financial and reputational impacts.

---

[3] This chapter avoids using the terminology 'Process Safety Management' (PSM), as this has a specific legal definition in some international jurisdictions.

[4] AIChE CCPS defines process safety as: *A disciplined framework for managing the integrity of operating systems and processes handling hazardous substances by applying good design principles, engineering, and operating practices. It deals with the prevention and control of incidents that have the potential to release hazardous materials or energy. Such incidents can cause toxic effects, fire, or explosion and could ultimately result in serious injuries, property damage, lost production, and environmental impact.* (CCPS, 2010, p. xvii.)

A wide range of hazardous materials and energies considered process hazards may lead to such serious consequences.[5] These process hazards and hazards traditionally the focus of generalist OHS professionals often occur together and, as part of role clarification, it is important to be able to differentiate the two types of hazard and so apply management strategies appropriate to the situation.

A member of the technical panel described his approach to differentiation:

> I like to explain process safety within a framework that considers *Process* (systems and risk process), *People* (including training and competency, human factors, leadership and culture) and *Plant* (inherently safer plant, layers of protection, design and operating limits, etc.). Plant aspects are (and should be) under the custody of process safety professionals or engineering capability. Process and People are often under the custody of an OHS professional (with many elements shared across the organisation), but with deference to process safety expertise relating to matters such as process hazard analysis, operator competency requirements, risk modelling and quantification, design that ensures safety and operating integrity (e.g. pressure relief valves, emergency shutdown systems and flaring design), risk-based inspection, testing and maintenance programs that ensure process plant integrity. Process safety professionals are also custodians of process safety knowledge and the development of sound process safety information (e.g. operations and maintenance procedures, process and instrumentation diagrams and schematics, hazardous area dossiers, process safety critical equipment, barriers and performance standards). (Chad Pettitt, personal communication, 4 March 2016)

## 1.3 Process safety vs OHS

Three key factors distinguish process safety from OHS:

- The mechanisms of causation – while both process safety and OHS are concerned with a potential loss of control of hazardous energy, process safety is usually about managing higher levels of energy
- The scale of potential consequences – while process safety incidents are less common than OHS incidents, their consequences are more likely to be severe
- The focus on engineering and design – process safety focuses on the safety of the system while OHS is about the safety of those who interact with the system.

Failure to identify these differences and develop appropriate management practices has been a significant factor in many process safety disasters.

However, there are similarities and overlaps. As identified by the IChemE Safety Centre (ISC, 2015a), managing process safety within an organisation requires leadership across functional elements of:

- Knowledge and competence

[5] See *OHS BoK* 17.4 Process Hazards (Chemical).

- Engineering and design
- Systems and procedures
- Assurance
- Human factors
- Culture.

This list could equally apply to OHS. Overlap with OHS can be identified in analyses of process safety disasters. For example, the following overlapping factors contributed to the 2005 BP Texas City refinery fire and explosion:

- Managers unaware of how work was being carried out (often referred to as 'work as done' compared with 'work as imagined')
- Cost and production pressures promoting deviations from documented procedures
- Limitations on maintenance due to cost pressure
- Priorities of managers directed by a corporate focus on cost and production
- Emphasis on people-focused controls
- Workers not understanding the process and the implications of changes in process parameters (job training)
- Workload and fatigue issues
- Risk-based decisions informed by invalid risk assessments based on incorrect assumptions
- Warning events being ignored (Hopkins, 2008).

Thus, there are opportunities for improving the management of both process safety and OHS through collaboration and shared learning.

Table 1 draws on an example of safe design of a liquefied petroleum gas (LPG) tanker to illustrate differences and similarities between the process safety professional and generalist OHS professional roles. There are aspects that require input of specific skills and knowledge, and areas of discipline overlap. An extended version of this table can be found in Appendix 2.

**Table 1: Comparison of process safety professional and generalist OHS professional roles using safe design of LPG tanker as an example**

| Concept | Process safety professional | Overlap | Generalist OHS professional |
|---|---|---|---|
| Safety in design, including systems | Integrity of tank and delivery hoses, excess flow valves, breakaway protection | Truck chassis design, load capacity, crash protection | Driver access to cab, posture issues in cab seating, weight and |

| | | | |
|---|---|---|---|
| | on hoses, pressure relief, tanker overfill safeguard, electrical immobilisation, interlocks, earthing integrity during load transfer | Site design, deluge cage design, gas and fire protection<br>Shared understanding of requirements to ensure 'fit for purpose' design | manoeuvrability of delivery hoses<br>Dashboard design |

# 2 Historical perspective

Many reviews of the history of process safety incidents focus on the last 50 years, typically commencing with the 1974 Flixborough disaster in England. Hendershot (2009) dramatically expands this scope by noting that, in the 14th century, Geoffrey Chaucer's *Canterbury Tales* described the explosion of a crucible in an alchemical process and the subsequent investigation.[6] The Industrial Revolution in the early 1800s is perhaps more appropriately seen as the beginning of the development of process safety in response to a number of steam boiler explosions. The onsite manufacture of nitroglycerine during the 1860s expansion of the US railroad is an early example of inherently safer design as it eliminated the risk to the public during transportation of nitroglycerine (Hendershot, 2009). Also during this period, Alfred Nobel's invention of dynamite by absorbing nitroglycerine onto an inert carrier to enhance its stability, provided another example of using a hazardous material in a less hazardous form (Hendershot, 2009).

Mannan (2012) explains the precursors to significant disasters in the chemical, oil and petrochemical industries that ultimately forced changes in the management of safety in these industries. Whereas prior to the 1960s chemical plants were usually small and could be started up and shut down with ease, during the 1960s:

> …process operating conditions such as pressure and temperature became more severe. The energy stored in the process increased and represented a greater hazard…At the same time, plants grew in size, typically by a factor of about 10, and were often single stream. As a result they contained huge items of equipment…and there was a high degree of interlinking with other plants through the exchange of by-products…These factors resulted in an increased potential for loss – both human and economic. (Mannan, 2012, p. 3)

Operation of such plants became complex and expensive, requiring high levels of engineering expertise to understand the process and to manage the process safely.

It is against this background that the 1974 Flixborough (Nypro, UK) chemical plant explosion killed 28 people, injured a further 89, destroyed the plant and caused widespread damage in the community. Key factors in the explosion are considered to be a lack of assessment of

[6] "The Canon's Yeoman's Tale"

the impact of temporary design changes during maintenance exacerbated by a lack of onsite expertise. The outcomes and subsequent investigation provided stimulus for widespread adoption of the first generation of process safety initiatives, which focused on management of change (MoC) in design, including the broader of systematic analysis processes such as hazard and operability (HAZOP) studies. Resulting site design developments included features such as safe location of buildings and use of blast-proof control rooms (Atherton & Gil, 2008; WorkSafe Victoria, 2020).

While the Flixborough event influenced the UK Health and Safety at Work etc. Act 1974, it was the 1976 Icmesa chemical company disaster in Seveso, Italy, that led to major regulatory change (da Cruz & Bentes, 2013). The Seveso Directive introduced outcome-based legislation requiring chemical facilities to demonstrate how they manage their operations safely – the safety case concept. The directive was amended to expand its scope in response to events such as the 1984 toxic release from a Union Carbide pesticide plant in Bhopal, India, and the 1986 Sandoz chemical factory fire in Basel, Switzerland, resulting in Seveso II in 1996. Following a cyanide spill (Baia Mare, Romania, 2000), a fireworks factory explosion (Enschede, The Netherlands, 2000) and an ammonium nitrate explosion (Toulouse, France, 2001), the scope of Seveso II was expanded to include storage and processing in mining and storage of pyrotechnics (Kerin, 2015). Seveso III was released in 2012; it included the community right to know and aligned Seveso with the Globally Harmonized System (GHS) of Classification and Labelling of Chemicals, now in it 7$^{th}$ edition (UN, 2017). Following the 1988 Piper Alpha (Occidental Petroleum) oil rig explosion, the outcome-based safety case legislation was extended to the offshore oil and gas industry. In Australia, the 1998 Esso Longford gas plant explosion had a profound effect, resulting in Victorian legislation for major hazard facilities based on Seveso II (Kerin, 2015), and influencing the creation of special units focusing on major hazard facilities by all state WHS regulators.

The Piper Alpha explosion also focused attention on the need for safe systems of work, particularly practices related to permit-to-work, isolation and lock-out tag-out procedures. The vital role of these procedures was apparent in a number of later disasters, including the 1989 explosions at the Phillips Petroleum chemical plant in Texas, and the 2001 explosion at a sulphuric acid tank farm at Motiva's Delaware City refinery (Atherton & Gil, 2008).

Poor management of change linked with limited or no availability of onsite specialist expertise is a consistent theme in analyses of process safety disasters. This deficiency can be linked to organisational culture, which is responsible for other features in the disasters. For example, at Bhopal, Union Carbide had the technology and process knowledge but left management and standard setting to the site management that was subjected to local pressures (Broughton, 2005; WorkSafe Victoria, 2020). The 1986 Chernobyl nuclear power plant explosion is often cited as the incident that elevated organisational culture into the mainstream of OHS discussion.

> A whole ‘safety culture’ concept arose after the Chernobyl incident, with strong support from the ILO [International Labour Organization]… [It] emphasizes a safety culture based on prevention and workers' participation. Lessons learned from Chernobyl not only had an impact on nuclear industries but also on other sectors, and launched a virtuous circle of improvements in all of them. (Niu as cited in ILO, 2006)

Corporate culture issues were seen to be at the core of factors leading to the 1998 Longford, Victoria, gas plant explosion (Hopkins, 2000; Nicol, 2001). The Longford incident also provides an example of other recurring themes identified in analyses of process disasters, including compromised design and maintenance of safety critical controls, actions associated with financial constraint and/or production pressures, and a personal safety focus at the expense of process safety (Atherton & Gil, 2008; Hopkins, 2000; Nicol, 2001).

Disasters such as the Longford incident, the 2005 Texas City refinery explosion, and the 2010 BP Deepwater Horizon explosion and oil spill at Macondo Prospect in the Gulf of Mexico contributed to the realisation that process safety cannot be measured using OHS accident data. Hopkins (2005) explains:

> Think about the airline industry for a moment. No airline in its right mind is going to try and convince the travelling public as to how safe it is by telling us its LTI (lost time injury) rate. The LTI rate is largely generated by baggage handling incidents, stress-related problems and so on. As members of the travelling public, we intuitively know that the LTI rate tells us nothing about the likelihood of an aircraft crash. The point is really obvious in that context. It ought to be similarly obvious in any major hazard environment.

In summary, the history of process safety disasters reveals a number of themes:

- Increasing technology, complexity and scale of plants
- Ad hoc development of regulatory frameworks
- Consequences of compromised site and plant design
- Link between design and maintenance of safety critical controls
- Need for safe work practices such as isolation and permit to work
- Importance of organisational culture, including management focus
- Impact of financial constraints and production pressures
- An incorrect assumption that process safety can be managed by the same strategies and metrics applied to personal safety.

An appreciation of this history provides useful context for understanding process safety and, importantly, draws attention to an apparent failure to learn from past events. Kletz observed as early as 1993 that:

> 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. Organisations do not learn from the past or, rather, individuals learn but they leave the

> organisation, taking their knowledge with them, and the organisation as a whole forgets. (Kletz, 1993, p. 1)

Hopkins (1999) expressed a similar view:

> Disasters are eminently preventable. They are not unforeseeable and unprecedented. In many cases the circumstances are disturbingly similar to those of earlier disasters. Too often they amount to 'carbon copies' of earlier disasters…This is what makes them so preventable. If only we had learnt and applied the lessons of earlier disasters the most recent of the series would have been prevented. (p. 157)

Subsequent publications by both Hopkins and Kletz reinforce this theme of a failure to learn,[7] as do the 2015 fire and explosion at a chemical warehouse in Tianjin, China, and the series of loss-of-containment events in 2015 and 2016 associated with Mexican state-owned oil company, PEMEX.

This was reinforced by Dame Judith Hackitt when she said:

> There are no new accidents just different people making the same mistakes because of a failure to recognise the relevance to them of other people's experience and therefore not learning.[8]

# 3 Extent of the problem

The consequences of a process safety incident can have catastrophic effects on people, the environment, facilities and equipment, and the reputation of organisations. Analyses of major disasters reveal that typically a complex interaction of factors leads to the incident and impacts on the outcomes (e.g. Hopkins, 2000, 2008, 2012; Kletz, 1985, 1993, 2003). These factors include what might be considered process safety failures as well as other factors. Notwithstanding this complexity, this section examines the extent of the problem from four perspectives: people, the environment, cost and business impact.

Australia has not been free of process safety incidents. In addition to the 1998 Longford explosion and the 2011 Laverton toxic release, which both resulted in fatalities (section 3.1), some serious process safety incidents in Australia have had the potential for disastrous consequences (Table 2).

---

[7] *Lessons from Longford* (Hopkins, 2000), *Failure to Learn* (Hopkins, 2008), *Disastrous Decisions* (Hopkins, 2012), *What Went Wrong?* (Kletz, 1985), *Lessons from Disasters* (Kletz, 1993), *Still Going Wrong!* (Kletz, 2003).

[8] 2022 Thomas Ashton Lecture (Hackitt, 2022), Taking the Blinkers Off [1]

**Table 2: Some Australian process safety incidents**

| Year | Type of installation | Location | Incident |
|---|---|---|---|
| 1989 | chemical plant | Seven Hills, New South Wales | fire |
| 1990 | LPG storage | St Peters, New South Wales | fire, tank explosion |
| 1991 | chemical storage | Coode Island, Victoria | tank explosion, fire |
| 2008 | upstream oil | Varanus Island, Western Australia | gas explosions, fires |
| 2009 | upstream oil | Montara, Timor Sea, north-west of Western Australian coast | explosion, oil and gas spill |
| **2019** | **Waste Facility** | **Campbellfield Victoria** | **Fire** |

## 3.1 People

By definition, process safety events have the potential for catastrophic loss of life. Table 3 lists 28 process safety disasters that resulted in a total of more than 5000 fatalities. This table includes only a small subset of all process disasters; also, it does not address the numbers of people injured, made ill, or otherwise impacted by these incidents and so severely underestimates human impact.

**Table 3: Some process safety incidents with associated fatalities since 1974**[9]

| Year | Location | Type of installation | Incident | Fatalities |
|---|---|---|---|---|
| **1974** | Flixborough, England | chemical plant | explosion | 28 |
| **1977** | Westwego, Louisiana, USA | Grain handling plant | dust explosion | 36 |
| **1984** | San Juanico, Mexico City, Mexico | LPG terminal | fire, explosions | >600 |
| **1984** | Bhopal, India | chemical plant | toxic release | >3000 |
| **1986** | Chernobyl, Ukraine (Russia) | nuclear power plant | explosions, fire | >30 |
| **1988** | Norco, Louisiana, USA | refinery | explosion | 7 |
| **1988** | Piper Alpha oilfield, North Sea | upstream oil | explosion, fire | 167 |
| **1989** | Pasadena, Texas, USA | petrochemical | explosions, fire | 23 |
| **1992** | LaMede, France | refinery | explosions | 6 |
| **1992** | Guadalaja, Mexico | gas pipeline | gas leak, sewer explosion | 252 |
| **1998** | Longford, Victoria, Australia | gas processing | explosion | 2 |

[9] Compiled from a number of references including Broughton, 2005 and Marsh, 2022.

| Year | Location | Type of installation | Incident | Fatalities |
|---|---|---|---|---|
| **2000** | Mina Al-Ahmadi, Kuwait | refinery | explosion, fire | 5 |
| **2001** | Campos Basin, Brazil | upstream oil | explosions | 11 |
| **2001** | Toulouse, France | chemical plant | explosion | 31 |
| **2003** | Chongqing, China | natural gas field | Explosion, toxic release | 243 |
| **2004** | Skikda, Algeria | gas processing | explosion | 27 |
| **2005** | Texas City, Texas, USA | refinery | explosion | 15 |
| **2005** | Mumbai High North Field, India | upstream oil and gas | fire | 22 |
| **2010** | Macondo, Gulf of Mexico | upstream oil | explosion | 11 |
| **2011** | Laverton, Victoria, Australia | chemical factory | toxic release | 1 |
| **2012** | Paraguana Peninsula, Venezuela | refinery | explosion, fire | 48 |
| **2014** | Soma, Manisa Province, Turkey | coal mine | explosion, fire | 301 |
| **2014** | Kunshun, Jiangsu, China | metal products factory | metal dust explosion | 146 |
| **2015** | Bay of Campeche, Gulf of Mexico | upstream oil | fire | 4 |
| **2015** | Tianjin, China | chemical storage | explosions | 173 |
| **2016** | Gazipour, Bangladesh | Plastic packaging factory | explosion | 33 |
| **2019** | Jiangsu, China | Chemical factory | explosion | 80 |
| **2020** | Beirut, Lebanon | Port storage | explosion | >200 |
| **2020** | Visakhapatnam, India | Chemical factory | Toxic release | >13 |
| | | | | **>5515** |

## 3.2 The environment

History records many catastrophes where process industries adversely impact ecosystems with widespread and/or long-lasting environmental consequences for agriculture, biodiversity, water sources and other natural resources. Table 4 demonstrates the severity of environmental impacts from a few process safety incidents.

**Table 4: Some process safety incidents and associated environmental impact**[10]

| Year | Location | Type of installation | Incident | Environmental implications |
|---|---|---|---|---|
| **1976** | Seveso, Italy | chemical plant | A runaway reaction in a chemical plant | Contamination of locally grown food, widespread death of animals; |

[10] (Compiled from a number of references including Broughton, 2005.)

| Year | Location | Type of installation | Incident | Environmental implications |
|---|---|---|---|---|
| | | | released 2,3,7,8-tetrachlorodibenzo-p-dioxin (TCDD) | emergency slaughtering of animals to prevent chemical entering the food chain |
| **1984** | Bhopal, India | chemical plant | An uncontrolled chemical reaction released methyl isocyanate gas and other chemicals | Broad-scale death of plants and animals created food shortages in the short term; long-term effects still impact plants, animals and people 30 years later |
| **1986** | Chernobyl, Ukraine | nuclear power pant | Overpressure led to steam explosion, fragmentation of fuel core and release of radiation | Contamination of the food chain resulted in a higher risk of cancer, death and reproductive loss in plant and animal populations up to 30 km from the site; strategies such as soil removal and exclusion zones were employed to mitigate the impact with the long-term effect determined by the half-life of the radionuclides; broader land contamination occurred with weather conditions and radioactive rainfall determining the level and range of contamination |
| **2009** | Montara, Timor Sea | upstream oil | Blowout and fire led to an oil spill that continued for 74 days, contaminating an estimated 90,000 $km^2$ of the Timor Sea | Oil and dispersants damaged coral and seaweed beds, impacting on fishing grounds with damage to mangroves putting villages at risk of flooding |
| **2010** | Macondo, Gulf of Mexico | upstream oil | Blowout of wellhead and release of an estimated 650 million L of oil into Gulf of Mexico | Described as the “worst environmental disaster in American history” by the US Natural Resources Defence Council (NRDC), the oil and dispersants had a devastating impact on marine plants (including death of seaweed beds), animals and birds, and severely impacted fishing and tourism |
| **2011** | Fukushima, Japan | nuclear power plant | A tsunami resulting from an earthquake struck the coast, impacting the power plant resulting in a meltdown, and release of radiation across a large area | Surrounding area remains highly radioactive, with some 160,000 evacuees still living in temporary housing; clean up estimated to take 40 years with some land unfarmable for centuries |
| **2014** | Charleston, West Virginia, USA | Chemical factory | A leak from a chemical storage tank entered the Elk River. | The Elk River supplies the drining water for the county. A mix of crude methylcychohexanemethanol |

| Year | Location | Type of installation | Incident | Environmental implications |
|---|---|---|---|---|
| | | | | (MCHM) and polyglycol ethers was released. |

Other examples of severe environmental impact from processes include river contamination from mining (e.g. Ok Tedi, Papua New Guinea, 1984-2006) and pipeline leaks contaminating surrounding land (e.g. Prudhoe Bay, Alaska, 2006).

## 3.3 Cost

An annual report on financial losses due to high-consequence incidents in the hydrocarbon industry estimated that the 100 largest losses between 1974 and 2021 amounted to US$48.482 billion adjusted to 2021 value (Marsh, 2022). The highest property loss event was the 1988 Piper Alpha upstream explosion in the North Sea (estimated US$2.384 billion) followed by the 1989 Phillips petrochemical explosion in Texas (estimated US$1.843 billion). Analysis of losses by sector found refining operations incurred 33% of property damage value followed by upstream 31%, petrochemicals 24% gas processing 8% and terminals 4% (Marsh, 2022).

While providing useful information, Marsh (2022) underestimates the costs associated with process safety incidents; not considered are uninsured losses such as regulatory fines, legal compensation costs or impact of reputational loss. Two examples give an indication of the potential further costs associated with process safety disasters:

- The 1998 gas plant explosion at Longford, Victoria, which caused property damage estimated at US$987 million adjusted to 2021 (Marsh, 2022), also resulted in Esso being fined A$2 million (ABC, 2018) and ordered to pay A$32 million in compensation to businesses that suffered property damage as a result of the incident (The Age, 2004) .
- While the property losses for the 2010 BP Macondo oil spill were estimated at US$782 million adjusted to 2021 (Marsh, 2016), BP also incurred a fine of US$20 billion and estimated the total cost of the disaster at US$61.6 billion (Burdeau, 2016).

Also, Marsh (2022) excludes the many process safety incidents of a smaller scale than the 100 most costly; these may well be significantly costly, threaten viability of an organisation and severely impact a community. Two examples of such prosecutions from the Victorian jurisdiction are:

- In 2012, uncontrolled release of gas from a pipeline during repairs with no injury, fine of $40,000 plus $14,000 costs
- In 2013, chemical exposure as part of herbicide manufacture resulting in a fatality, $300,000 fine (WorkSafe Victoria, 2012-24).

## 3.4 Other business impacts

Process safety incidents may also impact business profitability, reputation and viability. For example, the 2010 Macondo explosion led to a very public questioning of BP CEO Tony Hayward by the US Congress following which Hayward lost his role as head of BP (Whitford, Burke & Elkind, 2011). Fourteen years on, BP shares still consistently trade lower than those of competitors Exxon Mobil, Shell and Chevron (Figure 1).


**Figure 1: Comparison of share prices for BP and three competitors post Macondo explosion (NYSE, 2016)**

The Australian company, McAleese Group, provides an example of the potential for business viability and reputation issues to be associated with process incidents.

---

**Cootes Transport, McAleese Group**

In October 2013, a Cootes Transport petrol tanker lost control in Mona Vale, NSW, collided with passenger vehicles and caught fire. Two people were killed and a further five injured (ABC, 2013). The truck driver was initially charged with dangerous driving; this charge was dismissed when the cause of the accident was accepted as defective brakes (ABC, 2016).

Cootes Transport had been purchased by the McAleese Group in 2012. The incident delayed the McAleese IPO (initial public offering) with McAleese subsequently listed on the ASX in late November 2013. Further ramifications saw Cootes vehicles subjected to unprecedented roadside inspections across Australia; authorities in NSW and Victoria issued hundreds of defect notices that included ineffective brakes, oil and fuel leaks, steering, axle, suspension and tyre defects (Cooper, 2014). The entire fleet was grounded several times due to these multiple major defects. After satisfying a government requirement to show cause in March 2014, Cootes was allowed to continue to operate in NSW (McAleese Group, 2014). However, by this time it had lost several haulage contracts.

> Defence counsel Stephen Russell said the crash and resultant discovery of the safety breaches had cost the company, part of the wider McAleese Group, contracts “in the millions” of dollars, as customers had “lost faith in the Cootes Brand”. (Cooper, 2014)

Reductions of the Cootes workforce (from 1150 to 470) and number of vehicles (from 960 to 460), were expected by the end of 2014 (McAleese Group, 2014). In August 2014, McAleese reported an EBITDA (earnings before interest, tax, depreciation and amortisation) of $85.3 million against an IPO prospectus proposing an EBITDA of $126.8 million; “a net loss of $63.6 million in its first year as a publicly listed company…included some $76 million of costs associated with the accident” (Wiggins, 2014).

On March 16, 2016 it was reported that “McAleese future hangs on financial restructure after $97m net loss” (Wiggins, 2016a). Five months later, McAleese called in voluntary administrators after a recapitilisation bid failed; shares last traded at 2.5c, after listing at $1.47 (Wiggins, 2016b).

Negative business and reputational impact may also arise from process safety incidents that do not have major impact on human or environmental health, but rather erode community confidence in the operation of process. The following example of a series of chemical leaks at an Orica plant in New South Wales highlights the potential impact of damage to community confidence.

---

**Orica Australia Pty Ltd (Kooragang Island)**
Between October 2010 and December 2011, a series of significant incidents occurred at Orica Australia facilities. On 8 August 2011, the most serious of these incidents – a leak of hexavalent chromium into the air and onto some onsite workers – occurred at the ammonia plant at Orica Kooragang Island, Newcastle, close to the suburb of Stockton. This resulted in an independent review (O’Reilly, 2011) and a parliamentary inquiry (NSW Parliament, 2012).

In November 2011, the NSW State Government ordered the shutdown of the facility at Kooragang Island, 24 hours after an ammonia leak resulted in the hospitalisation of two people (Sikora, 2011). Head of the NSW Environment Protection Authority (EPA), Greg Sullivan, described the performance of Orica as “unacceptable …both the regulator and the community need to have confidence they [Orica] can operate that plant safely” (Sikora, 2011).

In December 2011, the EPA allowed Orica to restart some of its Newcastle operations (AAP, 2011). The day after the restart, about 20,000 L of a low-hazard substance was spilled, prompting a quick reaction by emergency services. While Orica and NSW Health said that the incident posed no risk to the surrounding community, a high level of community concern was reflected in media coverage:

> A Stockton resident says explosives maker Orica's emergency warning system for its Newcastle plant is not good enough…resident Rick Banyard says he was notified by Orica about the incident an hour after hearing it from someone else in the community…“Here we have the first time the warning system is going to be used and it's clearly failed," he said.
>
> Stockton residents group president Kate Johnson says if Orica is trying to regain the community's trust, it is failing miserably. “It does seem to be a bit of a circus,” she said. “I mean it seems to be that it’s an ailing plant that the plant management there just don't seem to be able to operate effectively. They haven't made it through 24 hours of operation so to me it seems like there doesn't seem to be control of the equipment that they have there."
>
> Minister for Environment, Robyn Parker, says while Orica notified the EPA about the spill immediately, another incident is unacceptable… “The community needs to have confidence in Orica and currently that confidence is very much shaken.” (ABC, 2011)

# 4 Legislation

Around the world, legislation that seeks to govern activities with process safety risks is either performance-based or prescriptive. Prescriptive legislative regimes, such as exist in the USA, have seen the emergence of specific standards[11] that provide useful benchmarks across jurisdictions. In Australia, New Zealand and European countries, a performance-based legislative regime requires high-hazard activities to be managed via regulated safety cases, in addition to general duties under OHS legislation that governs all workplaces.

The Australian regulated safety case approach, enshrined in specific legislation for major hazard facilities, emerged in response to Cullen's (1990) report on the Piper Alpha inquiry and was further informed by the Seveso Directives from Europe (EC, 2015). A safety case regime requires analysis and documentation detailing all hazards that could lead to a major incident, implementation of control measures to prevent or mitigate these hazards, provision of a safety management system and ongoing monitoring of the efficacy of control measures. Figure 2 outlines the safety case process. An essential element of such performance-based regimes is that the facility or company must identify relevant standards and processes to reduce safety risks so far as is reasonably practicable (NOPSEMA, 2022).[12]

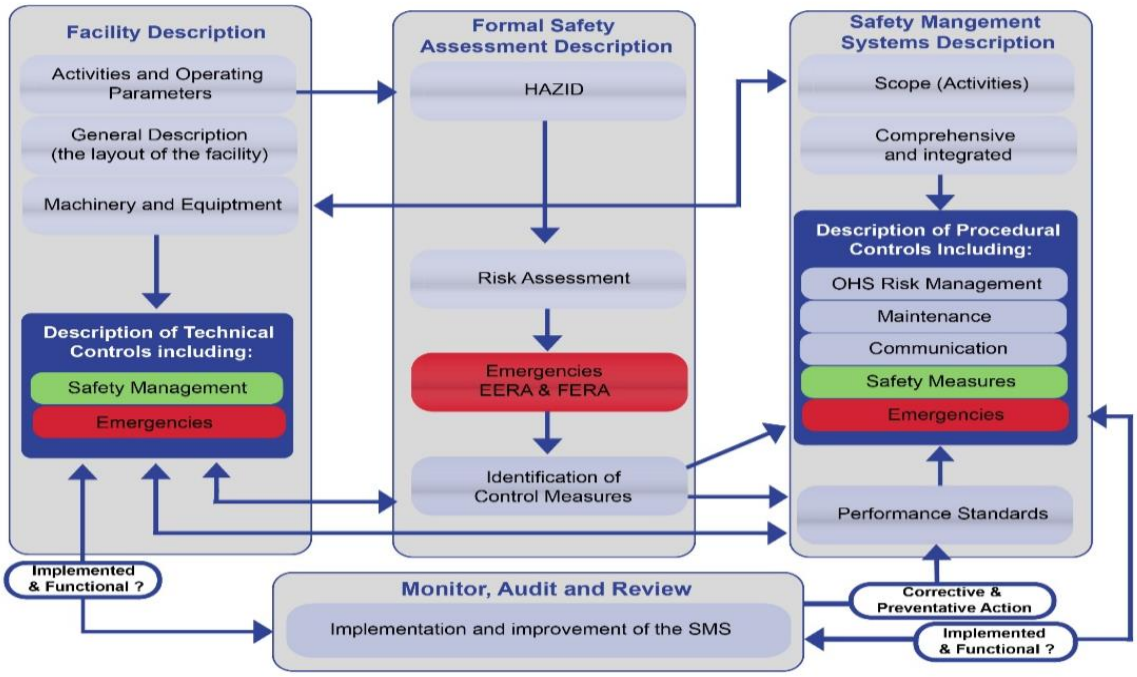



**Figure 2: The safety case process (modified from NOPSEMA, 2022, p.13)**

[11] e.g. *29 CFR 1910.119 Process Safety Management of Highly Hazardous Chemicals* (OSHA, 2000).

[12] See *OHS BoK 9.2* WHS Law in Australia for a discussion of the interpretation of 'reasonably practicable'.

Safe Work Australia describes major hazard facilities (MHFs) as:

> …locations such as oil refineries, chemical plants and large fuel and chemical storage sites where [quantities of hazardous materials above quantities as prescribed in legislation] are stored, handled or processed. Operators of determined MHFs have obligations to:
>
> - Identify all major incidents and major incident hazards for the facility
> - Conduct and document a safety assessment in relation to the operation of the facility that involves a comprehensive and systematic investigation and analysis of all aspects of risks to health and safety that could occur in the operation of the MHF
> - Implement control measures that eliminate or minimise the risk of a major incident occurring at the MHF
> - Prepare an emergency plan
> - Establish a Safety Management System (SMS) for the operation of the MHF
> - Prepare a Safety Case for the MHF that demonstrates that the MHF's SMS will control risks arising from major incidents and major incident hazards and demonstrates the adequacy of the measures to be implemented by the operator to control risks associated with the occurrence of major incidents. (SWA, 2012)

It is important to note that process hazards also exist at sites not deemed to be MHFs. In this situation, it is likely that a facility or organisation may not have process safety professionals employed. Consequently, it is vital that generalist OHS professionals recognise the hazards and access appropriate resources in managing the risk (e.g. NSW Department of Planning, 2011).

The performance-based safety case regime differs from the prescriptive regime in countries such as the USA where standards are established and mandated, and there is little encouragement to seek new and better standards to drive continuous improvement in safety outcomes. Performance-based regimes are considered to provide more opportunity to adapt to best practices and changing technologies, and to tailor individual systems. Consistent with the Robens (1972) principles that apply to all OHS law in Australia and New Zealand, the responsibility for safety is primarily on the organisation as the creator and operator of the risk.[13]

The investigation following the 2009 Montara oil rig blowout and subsequent fire and oil leak into the Timor Sea led to the expansion of the National Offshore Petroleum Safety Authority (NOPSA) into the National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA), which has jurisdiction in Australian Commonwealth waters, or waters where the states and territories have conferred powers (NOPSEMA, 2019). NOPSEMA is the first regulator in the world required to provide oversight of a performance-based regime for health, safety and environmental regulations across multiple jurisdictions. The complexity in regulating facilities from process safety and environmental perspectives across these

[13] See *OHS BoK* 9.2 WHS OHS Law in Australia for discussion of general duties under Australian model WHS legislation.

multiple jurisdictions can sometimes result in conflicting requirements, a challenge that must be managed effectively to ensure compliance with required legislation (NOPSEMA, 2019).

## 4.1 International perspectives

There are two main styles of legislation used to manage process safety internationally. They ca be described as: performance based and prescriptive. Additionally there are some jurisdictions that as yet do not have process safety specific legislation, such as Canada. The Australia model is aligned to the performance based style. This type of regime described the outcome required, allowing the facilities to define how they will achieve the outcome. Other jurisdictions that use this sort of model include the UK, European Union, Singapore, and New Zealand. Jurisdictions that have prescriptive based regimes include the United States. This type of regime defines specific requirements that must be met, as opposed to the outcomes.

# 5 Clarifying roles

Process safety professionals typically have a background in engineering with knowledge of process operations and plant equipment. Generalist OHS professionals come from a range of backgrounds that may include engineering, technical or science disciplines, but also health or other disciplines. While there are some undergraduate degrees in OHS in Australia, the current tendency is for OHS professionals to gain qualification through postgraduate study in the discipline of OHS.

Process safety and, to some extent, safety generally have suffered from the siloed approach of the process safety and OHS professions and structures within corporate management. Silos may arise for a range of reasons, including differences in professional 'culture', levels of technical knowledge and specialist language. An organisation's structural arrangements, internal politics, and lines of reporting and communication may also inhibit cooperation between the disciplines of process safety and OHS (e.g. Hopkins, 2012). Examples of the impact of siloed approaches to process safety and OHS are highlighted below.

**Example of silo approach: process safety impact on OHS – pump trailer**

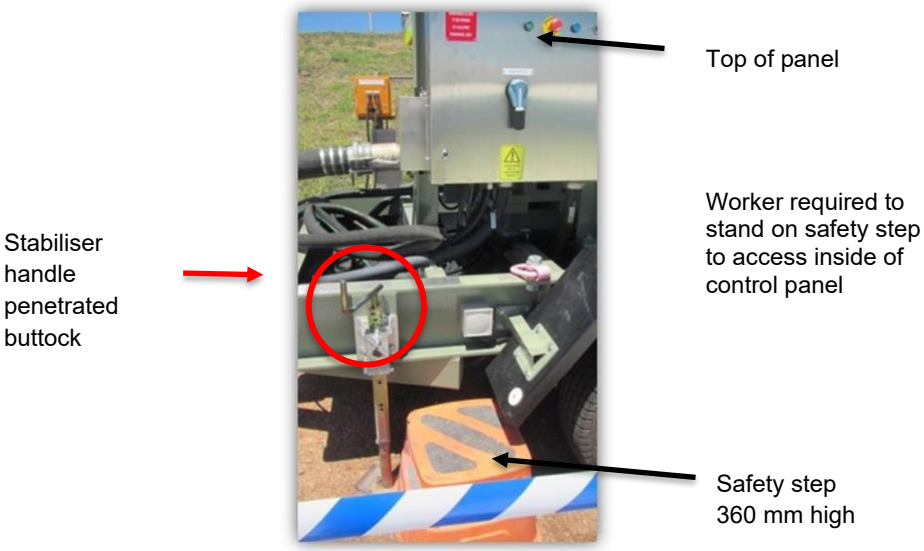
A pump trailer that had been in storage for several years was being commissioned to move water from one pond to another, over the crest of the two ponds where there was no fixed pumping. The trailer had been designed by company engineering staff with the fabrication outsourced. As part of commissioning, the operator required access to the internals of the electrical panel, which required use of a 'safety step'.

Commissioning of the pump trailer took three weeks. During this period, stabilising arms were added to the trailer to prevent the pump tripping due to the low tolerance threshold of the pump system (a process safety driven decision). Several hazard assessments were conducted, including design review, HAZOP, piping and instrumentation diagram, Operational Plant Risk Assessment, audit of as-built documentation, Job Task Risk Assessment and a personal Take 5. However, these assessments

did not take into consideration human factors such as the location and height of the control panel, and operational use and maintenance of the trailer.

At one point the worker stepped off the 'safety step', rotating 90 degrees and inadvertently positioning his left buttock over the stabilising handle (18 mm diameter, 125 mm long), which penetrated his buttock.

The personal safety hazard introduced by the stabiliser handle and the penetration risk of working above the stabiliser handle were not identified during the course of the various design and hazard reviews.




**Example of silo approach: OHS impact on process safety – tank farm maintenance**

*The company*

A multinational company with 20 manufacturing sites around the world; head office includes a central HSE department with one process safety professional.

*The site*

Produces resins, paints and coatings. A small management team includes a health, safety and environment (HSE) manager (responsible for HSE and some general production-related tasks) who does not have a process safety background, but has participated in some site HAZOPs. The plant is under financial pressure and all budgets, including maintenance, have been cut.

A range of hydrocarbon solvents are stored in small-to-medium-sized vertical fixed-roof and horizontal tanks with the vertical tanks 3-4 m diameter and 8-10 m high. Typical ambient conditions are such that tank temperatures are always well below the flash point of the solvents.

A hotel, a large shopping centre, and some offices and houses are located within a few hundred metres of the site.

*Site tour*

Stairways, ladders and platforms linking all the tank tops are badly corroded and have been barricaded. There is no plan to fix them due to budget cuts. Operators and instrument technicians are not allowed to access the roofs of the tanks as it is deemed unsafe. Some (but not all) of the level gauges are still functioning, but there is no way for the operators to check them by manually dipping the tanks even though this is a requirement in their operating procedures. Some of the tanks have high-level switches for alarms, but no one knows if they work; besides deliberately overfilling the tanks, there is no way of testing them.

The decision to barricade access to the tanks has been made for good 'personnel' safety reasons; they were clearly unsafe. However, the impact on process safety risk – the possibility of an overflow and/or a fire, internal tank explosions and multiple 'rocketing' tanks – and the possible impact on the neighboring population has not been identified.

Although the HSE manager and the site team are well aware that the high-level alarms are safety-related, there is no understanding as to how important the level instruments and alarms are, and how not maintaining them vastly increases the likelihood of a major event and the site risk profile.

---

**Example of silo approach: OHS impact on process safety – UV and heat protection for workers**

*The work area*

At a facility storing liquefied petroleum gas (LPG) workers are required to check and fill gas cylinders, ranging from 9 kg barbeque cylinders to 500 kg cylinders used for commercial purposes. There is a an LPG decanting tank used to empty cylinders of any remaining gas together with several stillages storing 9 kilogram LPG cylinders.


*The OHS hazard*

The work occurs in an open area with workers exposed to UV and heat stress.

*The OHS solution*

A shade sail manufactured from synthetic material was installed to cover the whole area. The shade sail was not part of the original design.

*The outcome*

A lack of collaboration and discussion on the various hazards in the area and deficient management of change processes resulted in a failure to recognise the process hazards of a combustible materials in the presence of flammable, dangerous goods, which can significantly change the escalation potential of a fire. Also, the shade sail was positioned above the pressure relief valve of the LPG decanting vessel, further increasing the risk.

*Corrective action*

Given the need for the shade sail in managing the heat stress hazard, the operator implemented risk control measures including for managing the process hazard including minimising the volume of LPG stored in the surrounding area and re-routing the discharge outlet of the LPG tank pressure relief valve outside the footprint of the shade sail. They also improved firefighting capability.

Effective management of both process safety and OHS requires collaboration across the two disciplines to facilitate understanding of the issues and perspectives of both professions and to arrive at solutions that address both process safety and OHS risk. For example, while it is not acceptable to leave a tank farm bund drain open and so allow uncontrolled drainage of potentially contaminated rainwater into the local water course, it is also not acceptable to allow the stagnant water in a bund to become a potential health risk (e.g. a breeding ground for mosquitoes with the associated health risks).

This chapter and the companion *OHS Body of Knowledge* chapter, 17.4 Process Hazards (Chemical), bridge the gap between the disciplines by equipping generalist OHS

professionals with basic process safety knowledge to inform their practice and facilitate collaboration with process safety professionals. They also serve to raise process safety professionals' awareness of the role of OHS professionals and the need to consider the OHS impacts of actions taken to improve process safety.

The IChemE Safety Centre has developed a process safety competency framework (ISC, 2018) that describes the competencies and proficiency levels for key roles in an organisation from, for example, operator, supervisor, project and general management, and support roles such as human resources to the board of management. Competencies are defined for process safety professionals and for generalist OHS professionals at both site and corporate levels. This structure allows identification of the respective roles of process safety and OHS professionals and areas of overlap. While not a definitive list, Table 5 compares some general distinguishing features. Appendix 2 provides a scenario example of the process safety and OHS roles in managing hazards associated with operating an LPG tanker. A supplementary guidance document was also written by the IChemE Safety Centre to explain how to build competence (ISC, 2020a).

**Table 5: Process safety professional and generalist OHS professional roles – some distinguishing features and areas of overlap**

| | Process safety professional | Overlap | Generalist OHS professional |
|---|---|---|---|
| **Focus** | Approach focused on high-consequence, low-frequency issues resulting in loss of control with potentially catastrophic consequences | Public and environmental impacts of the operations | Main focus on workers, impact of process on person<br>Emphasis on management systems |
| **Risk management** | Hazard identification based on detailed, systematic analysis | Similarity in fundamentals of hazard identification and risk assessment<br>Concept of the hierarchy of control | Hazard identification based on a range of information, including consultation with stakeholders |
| | Risk assessment focus on operational risks associated with process and equipment | Warning signs of potential loss of control.<br>Awareness of consequences of loss of control | Workplace risks associated with the work undertaken by people or that impacts people |
| | Quantitative risk assessment | Semi-quantitative risk assessment | Qualitative risk assessment processes<br>Hazard-specific quantitative risk assessment |
| | Risk to community, workers and the facility | Risk to the environment | Risk to workers |
| **Emergency preparedness** | Predictive analysis, e.g. consequence modelling | Preparedness of systems response | Focus on personal safety |

| | Process safety professional | Overlap | Generalist OHS professional |
|---|---|---|---|
| | Focus on containing the process | Environmental impact of emergencies and emergency response; recovery after emergency | |
| **Engineering & design** | Design and hazard analysis to inform and support inherently safer process plant | Plant/operator interface | Structures, materials and plant/equipment with an emphasis on plant life cycle and worker safety |
| **Asset integrity – inspection & maintenance** | Integrity of critical controls<br>Equipment reliability | Condition monitoring | Inspections and maintenance schedules |
| **Management of change (MoC)** | Engineering and technical change, temporary design or operational changes<br>Consistent, up-to-date documentation | Resolution of potential issues from changes to plant, equipment, process or people<br>Managing people through change via communication and consultation | Changes having an impact on the organisation of work, the environment or standards impacting work. May be organisational, legislative or other sources. |
| Systems & procedures | | Systemic and systematic management approach | |
| **Safety systems analysis** | Evaluation of process safety MS effectiveness and reliability of barriers<br>Process safety performance metrics | Systems review | Evaluation of OHS MS effectiveness and risk controls<br>OHS performance indicators |
| **Systems manuals & drawings** | Accuracy of technical information and drawings | Documentation review | Currency of documentation relating to worker safety |
| **Process monitoring & handover** | Operating process within design envelopes<br>Communication of process safety critical information | Channels of communication about safety | Effective shift handover process, particularly in maintenance |
| **Operational interfaces** | Communication of process safety critical information across interfaces | Third party process interfaces such as supplier specifications | Effective consultation on safety issues between operators, managers and other relevant staff |
| **Contractor & supplier selection & management** | | Contractor competence | Contractor personnel safety |
| **Root cause analysis** | | Systematic analysis processes | |
| **Management of Safety Critical Elements** | Ongoing integrity and reliability | | |

| | Process safety professional | Overlap | Generalist OHS professional |
|---|---|---|---|
| **Reporting & investigation** | Reporting of process deviations | Legal requirements for reporting<br>Analysis to identify trends<br>Learning from experience | Incident and injury reporting |
| **Legislation, regulations, codes and standards** | Focus on specific duties assigned in legislative requirements for high-hazard activities | Environmental legislation | OHS specific legislation |
| **Audit, assurance, management review and intervention** | Audits of asset integrity against engineering standards | Management systems audits | Hazard and compliance audits on plant, equipment, chemicals, asbestos, training, housekeeping procedures and behaviours |
| | Continuous review focuses on systemic root causes | | Improvement processes focus on both immediate and latent causes |
| **Human factors** | Impact of the person on the process and integrity of the system | Interaction of the person, task and organisation | Impact of the process on the person |
| **Organisational culture** | | Safety leadership and commitment<br>Communication channels | |

# 6 Hazard identification and risk assessment

Active participation in process hazard identification and risk assessment requires underpinning knowledge and skills relating to:

- Chemical and physical characteristics of hazardous substances, including chemical incompatibility and descriptive parameters such as lower flammable/explosion limit (LFL/LEL), upper flammable/explosion limit (UFL/UEL), autoignition temperature (AIT), flash point, fire point and toxicity measures such as $LD_{50}$
- Potential mechanisms and consequences of a loss of control
- Reading and understanding basic engineering drawings
- Failure modes and rates
- Various process hazard identification and risk assessment tools and the potential for the generalist OHS professional to contribute to use of such tools.

Chemical and physical characteristics and consequences of loss of control are addressed in the *OHS Body of Knowledge* companion chapter 17.4 Process Hazards (Chemical). The following sections discuss relevant engineering drawings, failure modes and rates, and hazard identification and risk assessment tools with emphasis on the contributory role of the generalist OHS professional.

## 6.1 Engineering drawings

While engineers use many types of technical drawings, those most relevant to the generalist OHS professional participating in process safety risk assessments are Process Flow Diagrams (PFDs), Process Safety Flow Schematics (PSFSs) and Piping and Instrumentation Diagrams (P&IDs).

The generalist OHS professional is not expected to be able to work in depth with such diagrams, but should be familiar with their use. Some suggestions for an OHS professional likely to be involved in a risk assessment or discussion based on a PFD, PSFS or P&ID are:

- Ask for a legend and explanation of symbols (different legends and/or meanings may apply in different organisations)
- Develop an appreciation for how the drawing reflects what is in the field. PFDs, PSFSs and P&IDs are not to scale. One strategy is to 'walk the lines' accompanied by an engineer or operator with the drawing in hand. Some questions while walking the lines might be:
    - What chemical is in this vessel/pipe?
    - What might happen if ...?
    - How is the integrity of the equipment managed?
    - How could cross-contamination of chemicals occur? What would happen if such contamination occurred?
    - How can we safely isolate this equipment for maintenance?
    - How can we safely access the equipment to maintain it?
    - In what ways are operators required to directly interact with the equipment?

**Figure 3: 'Walking the lines'**
(image courtesy of Origin Energy)

### 6.1.1 Process Flow Diagram

A Process Flow Diagram (PFD) is a logic diagram showing major items of equipment and how they relate to the process route (Figure 4). It usually indicates significant process piping, major equipment (pumps, vessels, heat exchangers) and control loops. A PFD is usually matched with a Heat & Mass Balance data table, which indicates mass flows, temperatures, pressures and compositional changes through the process.

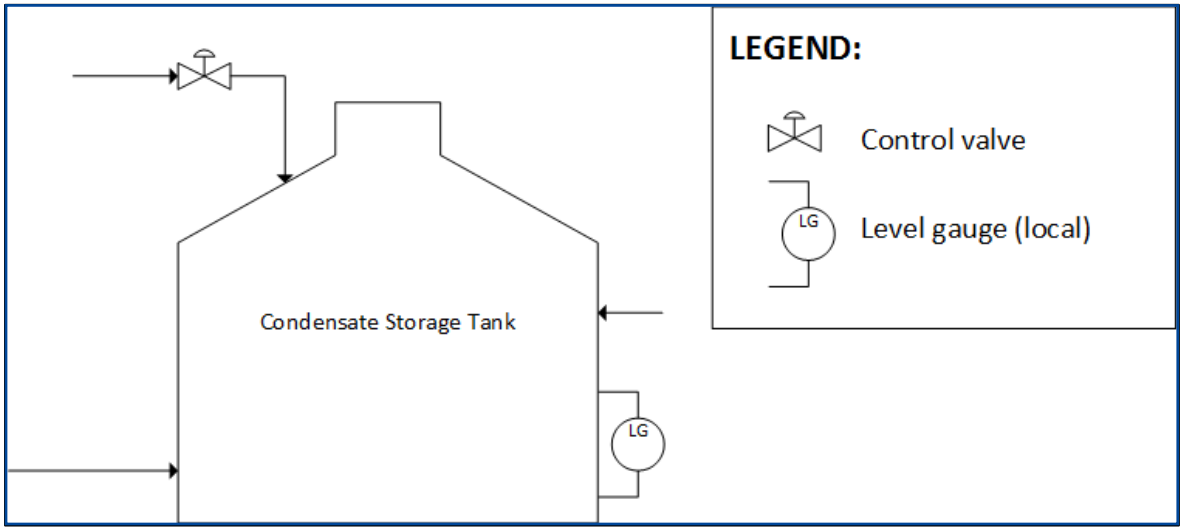



**Figure 4: Example of a simple PFD**[14]

### 6.1.2 Process Safety Flow Schematic

PFDs are frequently used as the basis for Process Safety Flow Schematics (PSFSs) on which process safeguarding equipment is shown (Figure 5). Such equipment includes trip sensors, emergency shutdown valves, pressure relief valves (PRVs), non-return valves, locked open/closed values, restriction orifices and excess-flow valves.

[14] Engineering diagrams courtesy of Ivica Ninic (Origin Energy) and Joe Aiken (Safety Solutions, NZ).

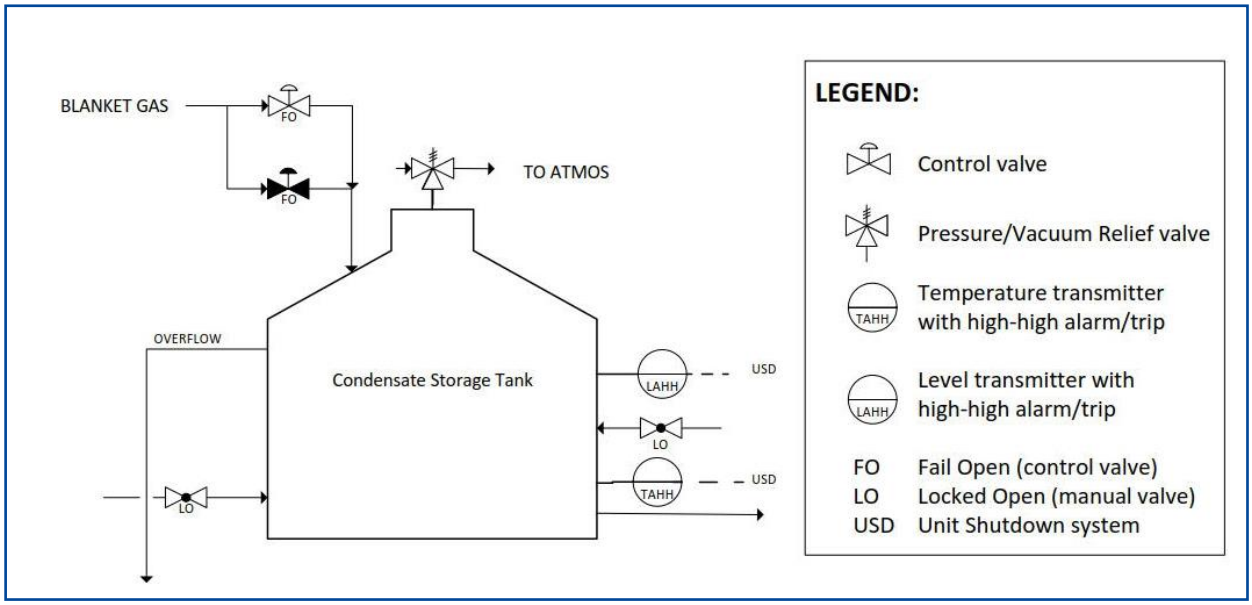



**Figure 5: Example of a portion of a PSFS**

### 6.1.3 Piping and Instrumentation Diagram

A Piping and Instrumentation Diagram (P&ID), historically called an Engineering Line Diagram (ELD), is the master drawing for a process plant (Figure 6). Typically, it covers one or more pieces of equipment and all related piping and control/safeguarding systems related to the equipment, and includes:

- A representation of the item(s) of pressurised equipment, showing piping and instrument connections with flow directions
- Basic operating and design data for the equipment
- Equipment and instrument tag numbers, line numbers, valve types and normal operating status with alarms and trip functions
- Piping size, class (pressure rating and material of construction), insulation and other key specifications
- Connecting links to other P&IDs for associated equipment.

P&IDs are used in engineering design and as a basis for risk assessments of the process operation, such as HAZOP. The diagram elements are indicative and not to scale; while they do not indicate spatial layout, the relative location of piping connections should be correct. This means that some relatively short lines on a P&ID could actually be metres long.

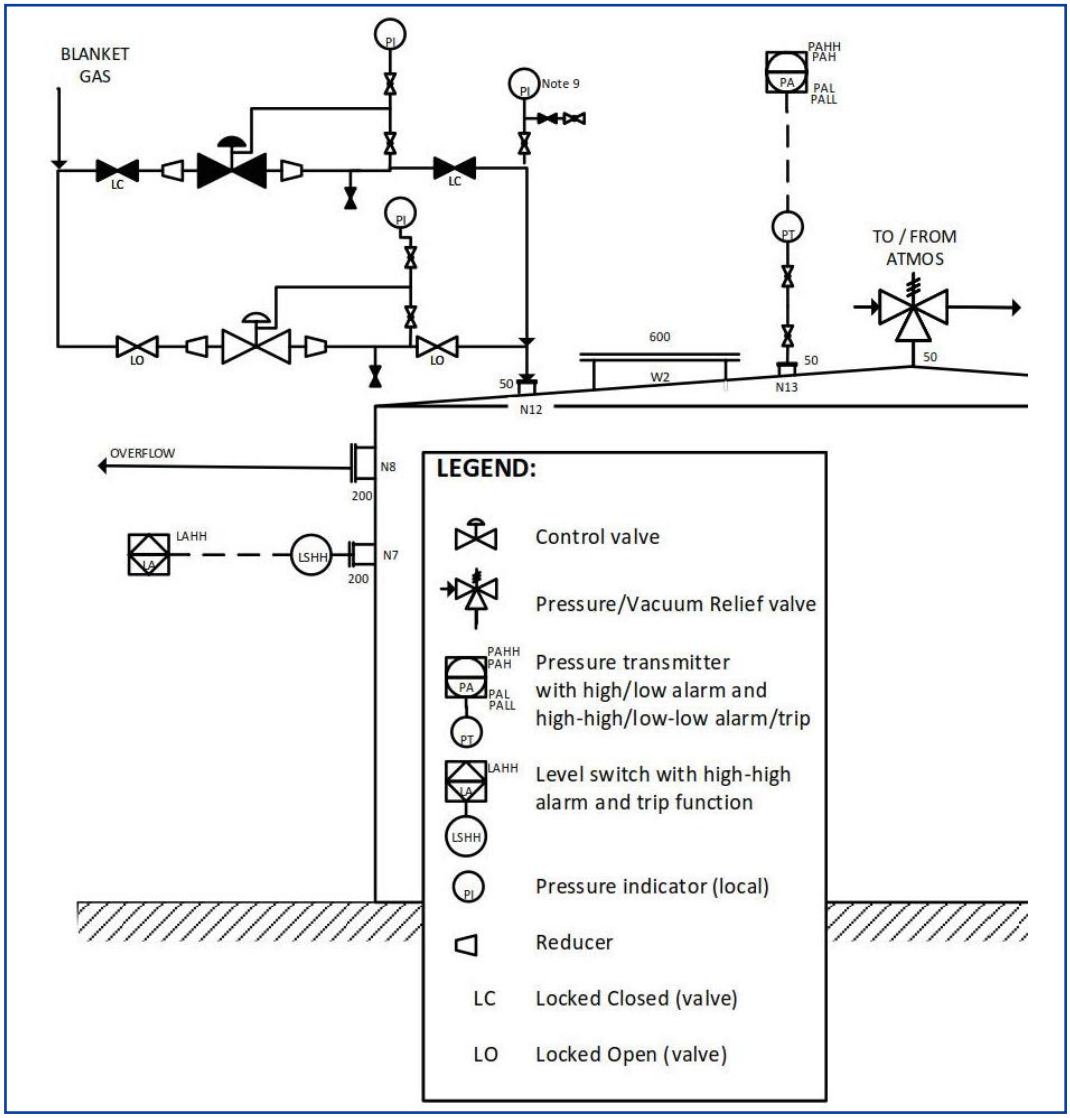



**Figure 6: Example of a portion of a P&ID**

### 6.1.4 Other engineering diagrams and documents

Other types of documents routinely used by process safety professionals in risk assessment or the presentation of safety cases include cause and effect diagrams, bowtie diagrams, fault trees, event trees, consequence-model diagrams and safety critical element (SCE) registers. The diagrams may be used to calculate and show the risks or consequences of an event while SCE registers are used to ensure there is a comprehensive list of items requiring monitoring and to connect the monitoring data to identify trends.

## 6.2 Failure modes and rates

Understanding the different modes of failure of equipment being risk assessed as well as the estimated frequency of such failures is essential for valid risk assessments.

### 6.2.1 Failure modes

Equipment may fail for a variety of reasons including but not limited to:

- Faulty manufacture
- As part of commissioning and early operation
- Operation outside design parameters.
- Deterioration as a result of wear, corrosion, etc.
- Poor or no maintenance.

The activities and management strategies within key elements of the OHS management systems important in identifying potential failures are:

- Inspection activities to identify
    - Significant corrosion, damage, leaks, etc., not only in parts of the plant itself but also in associated equipment and structures
    - Gauges reading outside normal parameters or damaged
    - Tank bunds containing significant quantities of water
    - Unusual process noises, vapour/steam cloud, temperature/dew
- System review to verify
    - Preventive maintenance occurs as scheduled
    - Inspections occur as scheduled and are findings addressed in accordance with risk
    - Management of change (MoC) processes robustly implemented
    - Personnel trained and competent to do their allocated work
    - Emergency preparedness, including ensuring local emergency services are fully briefed on process hazards
    - Identification of potential adverse impacts from thunderstorms, cyclones, floods other natural disasters, loss of power, industrial action and cyber interference, and preparation for such events.

### 6.2.2 Failure rates and reliability

When managing process safety risks it is often necessary to quantify the failure rate of equipment that can result in a loss of control or containment of a hazard (e.g. number of seal failures per year) and of the safety equipment designed to prevent or mitigate the hazardous event (e.g. probability of high-level trip on tank not working when required). Similarly, failure

of procedures, often due to people making mistakes, can impact on process safety in the same two ways.

Failure rates of equipment or procedures that can lead to loss of control or containment of a hazard allows the *initiating event* frequency to be calculated. This is always reported as a failure rate per unit time, typically events/year. Examples of these types of failure rates are the number of seal failures per year, or an estimate of how many times per year an operator may line up the run-down into the wrong tank. Both examples are typically known as primary causes of a hazardous event or scenario, because they are the initiating step that begins the scenario developing; and will lead to the incident, if not prevented or mitigated by suitably designed safety systems.

Equipment or systems designed to prevent or mitigate the incident are known as *layers of protection*. These may include hardware such as pressure safety valves or a high-level trip on a tank; together with operating procedures describing the required response to an alarm. The failure probability of equipment or systems designed to prevent or mitigate the hazardous event (i.e. layers of protection) is known as the probability of failure on demand (PFD) and is a dimensionless number with a value of zero to one (e.g. probability of a high-level trip on a tank not working when required).

The primary difference between the initiating event and the layer of protection is that the initiating event 'causes' the hazardous scenario to start whereas the layers of protection stop it from developing.

Determining failure rates and probabilities requires quality data and an understanding of reliability mathematics.[15] Failure rate data is typically unavailable within most organisations and is rarely available from component manufacturers. Engineers normally use standard industry tables[16] to estimate failure rates and probabilities backed up with on-site operating experience of the particular equipment and location when this is available. The same equipment may fail in a number of ways; only some of which may lead to the loss of control or failure of the safety system, so it is important that any data used is interpreted carefully. Some larger companies issue internal guidance on what failure rate data and probabilities should be used, but even these should be used with care.

[15] For an overview of reliability mathematics and failure see Chap 9 in Viner (2015).

[16] e.g. See Safety Equipment Reliability Handbook (Exida, 2015) Process Equipment Reliability Database. (PERD) (CCPS, 2017).

Reliability mathematics can be quite complex and various techniques are available to perform the calculations. For some complex situations, especially when there is a high or perceived high underlying risk or consequence, detailed Fault Trees and Event Trees may be developed. For simpler systems a simplified technique known as layers of protection analysis (LOPA) may be used. [17]This is a technique that has come into widespread use in recent years and is preferred by many regulators as it balances ease of use with a reasonable degree of rigor.

For Safety Instrumented Functions (SIF) such as trips and interlocks, Safety Integrity Level (SIL) analysis is performed to determine the required reliability of the system. This is known as S*IL Assessment* or *SIL Determination*. This is typically led by process safety professionals with input from a multi-disciplinary team including process engineers, operations personnel, instrument and control engineers and generalist OHS professionals. It is a form of risk assessment as the exercise is aimed at determining the required layers of protection to achieve a required risk target. The most common methodology for performing SIL assessment studies is LOPA in which each hazard is considered, existing controls (layers of protection) are examined and a gap is identified to achieve the target risk level. The SIF PFD and SIL is then specified to close this gap. It is important that each layer of protection is independent of each other and from the initiating cause. Both the SIL and the required probability of demand must be specified for the SIF to be designed; it is possible for the SIF to meet the SIL requirement but not to meet the PFD requirement.

The target risk level is typically company specific and varies across organisations depending on their risk appetite and the approach by the relevant regulator. The target risk level applies per loop or system under consideration and differs from a company's overall individual risk criteria, typically by an order of magnitude. This is because any individual would be exposed to multiple risks whereas the LOPA calculation applies only to a single incident or risk. For different potential consequences (multiple fatalities, single fatality, serious injury, etc.), there may be different target risk criteria and so different reliability requirements. Meeting the target risk level does not necessarily mean that the risk is managed 'so far as is 'reasonably practicable'; additional controls may be necessary to achieve this legally required standard.

The design of SIFs and their components must be checked (verified) and if the failure rate does not meet the PFD requirements, then more reliable components, different configurations or additional devices may be needed. Once the equipment is installed and operated it must be checked again (validated) to ensure it meets the specified design requirements. Verification and validation is usually performed by specialist instrument and control engineers. Just as importantly, the SIF must be maintained and tested throughout its lifetime to ensure it meets the required reliability during ongoing operation.

[17] See *OHS BoK* 17.4 Process Hazards (Chemical).

### 6.2.3 Independence of protection systems

When identifying failure modes or when undertaking a SIL study, it is important to identify the independence or linkage of potential failures. If a backup or separate protection system has a similar failure mode, and these can be linked in an actual failure, it is not independent and the protection may not work as required. For example, a high-level alarm and a high level shut down trip, both reading from the same level sensor are not independent as they have a common mode of failure, the high-level sensor. Independent operation would require a separate sensor for the high-level shutdown trip. Independence could also be traced further, for example, if both sensors were powered from the same source, the level of independence is reduced.

This independence, or otherwise, is demonstrated using AND / OR logic in failure modelling such as Fault Trees. When using LOPA, multiple layers that are not independent are typically discounted and only one layer is credited.

### 6.2.4 Organisational and human factors

Because process safety and OHS occur within a *sociotechnical system*, the relationships of workers with each other, with management and with the technical system must be considered as a functioning whole.[18] Thus, while process safety has a focus on technical analysis and engineering design, this must consciously be placed in the context of the organisation taking account of the operators and other key personnel. Furthermore, technical performance is influenced by management decisions, organisational and safety culture, and external sociopolitical pressures (Reason, 1997).[19]

Human factors play a major role in process safety incidents and in the management of process safety. An understanding of human factors and organisational impact on human behavior and response is vital in considering modes of failure; this approach is quite different to a focus on humans as the source of the problem or error.[20]

Kletz (2001) identifies ‘errors’ in engineering and process safety events, including:

- Simple slips (e.g. forgetting to open/close a valve, error in calculation, wrong connection, failure to notice)

---

[18] See *OHS BoK* 12.1 Systems for discussion of sociotechnical systems.

[19] *OHS BoK* 10.1 The Organisation and *OHS BoK* 10.2 Organisational Culture discuss these organisational and cultural factors.

[20] *OHS BoK* 34.3 Health and Safety in Design discusses factors impacting on the human-equipment interface. See also *OHS BoK* 8 series of chapters on psychology.

- Errors related to training or instructions (e.g. knowledge of what we don't know, inappropriate reliance on training, contradictory instructions)
- Failure to follow instructions (including non-compliance by managers and operators)
- Errors in design and/or construction (e.g. faulty conceptual design, pipe failures, contractor issues)
- Maintenance errors (lack of understanding of how equipment works, incompetence, short cuts, poor maintenance practices)
- Operational and communication errors (e.g. inadequate use of permit-to-work systems)
- Errors in computer-controlled plants (e.g. software errors, entering wrong data, misjudging response by computer, changes to programs without management of change)
- Errors related to management environment (including cost and production pressure).

However, Kletz (2001) challenges the value of talking about human error as a cause and suggests focusing on the action required to prevent the 'error' occurring. This approach is taken up by Dekker (2006), who explores 'old' and 'new' views of human error. While the old view attributes error to mishap, the new view sees it as symptomatic of deeper trouble and, rather than focusing on where people went wrong, advocates finding out "how people's assessments and actions made sense at the time, given the circumstances" (Dekker, 2006, p. xi). Characteristics of the new view of human error are based on the concept of work as a sociotechnical system and resonate in a process safety environment:

- Complex systems are not basically safe
- Complex systems are trade-offs between multiple irreconcilable goals (e.g. safety and efficiency)
- People have to create safety through practice at all levels of an organization (Dekker, 2006, p. xi).

## 6.3 Approaches and tools

Hazard identification and risk assessment are core activities for both the process safety professional and the generalist OHS professional. While these activities are similar in concept for both OHS and process safety, they differ in the detail and, in some cases, the types of tools used. This section focuses, firstly, on these differences in approaches to risk assessment and, secondly, on types of process safety analysis and the potential contributory role of the generalist OHS professional.

### 6.3.1 Differences in risk assessment approaches

While the objectives of OHS and process safety risk assessments are similar, some key differences in approach can be considered under the headings of:

- Focus
- Hazard identification
- Risk assessment tools
- Inputs
- Outcomes.

#### Focus

The most obvious difference between OHS and process safety risk assessments is the focus of the assessment. OHS risk assessments tend to focus on worksite risks associated with the work undertaken; they assess the risk to the worker/s due to the work, plant and equipment, materials and work environment (e.g. heights, confined spaces, work practices, external impacts). Process safety risk assessments focus on operational risks associated with the process equipment and assess the risk to the facility, workers and the community.

#### Hazard identification

While specific 'sources of potentially damaging energy' may be considered the hazard in both OHS and process safety studies, the method of identifying their presence and action differs. Generalist OHS professionals gain information through observation, experience and data, and process safety professionals also employ hazard identification techniques such as Process Hazard Review (PHR) and HAZOP studies that feature guidewords.

#### Risk assessment tools

There are three main types of hazard identification and risk assessment tools:[21]

- *Qualitative* – using matrices and hazard identification techniques featuring guidewords
- *Semi-quantitative* – where word descriptors are associated with numerical ratings. For generalist OHS professionals, these may include matrices with numerical risk ratings, spreadsheet assessments and nomograms; process safety professionals may use LOPA or SIL analysis.
- *Quantitative risk assessment* (QRA) – based on detailed consequence modelling and frequency analysis (e.g. using fault trees and event trees).

  While quite different to QRA, risk assessment tools with a numerical basis are used by generalist OHS professionals, e.g. hazard-specific tools for measuring exposure to chemicals, force and related risks associated with manual handling, biological

[21] See *OHS BoK 31.1 Risk* for a discussion on the various types of risk assessment.

indicators to assess fatigue, and surveys and tools to assess risk from psychosocial hazards.

### Inputs

Generalist OHS professionals base risk assessments on a broad range of information and data, including the history of incidents inside and outside the company, legislation and standards, industry information, observation and expert opinion. Process safety professionals use such information in addition to equipment failure rates, process parameters and engineering-based calculations.

Consultation is a legislative requirement under Commonwealth and state work health and safety legislation.[22] Both generalist OHS professionals and process safety professionals seek input from key stakeholders, including those who do the work and those who may be affected by the work process. Such consultation has a higher profile in risk assessments by OHS professionals; for process safety professionals, risk assessment is a more technical process.

### Outcomes

For both OHS and process safety, the objective of risk assessment is to understand the nature of the risk to inform development and implementation of controls. The key differences are in the focus and nature of the controls. Process safety controls, primarily focus on protection of the plant and operations, are commonly engineered controls (e.g. alarms, trip systems and relief valves) supported by administrative controls (such as permit to work and competency). OHS controls mainly focus on worker protection with the nature of the controls implemented based on:

- Need for requisite variety to address complexity
- Effectiveness of control as indicated through hierarchies of control
- Time sequence for employing controls
- Sociotechnical environment in which the control will operate.[23]

## 6.3.2 Types of process safety analysis

There are many different types of risk assessment techniques used in process safety. Table 6 outlines a range of tools in general use and identifies the role of the generalist OHS professional in the use of each tool. This table does not include tools commonly used by both OHS and process safety professionals (e.g. bowtie diagrams).

---

[22] e.g. SWA, 2023b, s49.

[23] *OHS BoK* 34.1 Prevention and Intervention.

**Table 6: Hazard identification and risk assessment tools used in process safety and their relevance to generalist OHS professionals (modified from IChemE, 2016)**

| Tool | What is it? | When is it used? | What should an OHS professional do? | Key words / specific knowledge |
|---|---|---|---|---|
| **Concept hazard analysis** | Qualitative method for identification of hazard characteristics; identification of areas recognised as particularly dangerous based on previous site and industry experience | As a screening tool to identify scenarios requiring further analysis | Contribute to the analytic discussion from the OHS perspective, taking account of industry history and experience | |
| **Hazard identification (HazId)**<br><br>**Process hazard review (PHR)** | Structured techniques to identify hazards that could affect an operating process plant; usually based on PFDs | To identify hazards in the initial stage of a risk assessment process | Identify non-process hazards that may interact with / contribute to the process hazards being assessed.<br>Contribute to the analytic discussion from the OHS perspective | Uses a top-down guideword approach based on generic causes or consequences |
| **Hazard and operability (HAZOP) study** | Structured technique performed by a multidisciplinary team to prompt a detailed analysis of process design to identify potential deviations from intended design and function | Can be applied to a wide range of complex systems, e.g. batch-plant operation, procedures, software development.<br>Usually used in early-design phase to identify potential design shortcomings and in detailed-engineering phase to review the completed design for issues that may have been missed in previous reviews | Contribute to the analytic discussion from the OHS perspective with a focus on safe operability of the process | Uses guidewords<br>Requires expert facilitation |
| **Consequence (dispersion) modelling** | Numerical process for estimating the spread of a released gas or liquid and the physical impact, which is presented in a numerical or graphical format | To determine the range and scale of potential consequences as part of risk assessment and emergency planning | Participate in interpretation of results and discussion of how results may impact people and the environment with a focus on broader community impact | Toxicity Emergency Response Planning Guidelines (ERPGs) (AIHA, 2016)<br>Often supported by modelling software |

| Tool | What is it? | When is it used? | What should an OHS professional do? | Key words / specific knowledge |
|---|---|---|---|---|
| **Fault tree** ***(examines causes)*** | Graphical representation of component failure modes and operator actions leading to a particular system failure; addition of frequencies and probabilities enables quantification of the top event | To analyse causes of an incident as part of developing prevention strategies | Interpret a fault tree to understand the likelihood of potential failure pathways | Starts with definition of top event, then definition of essential conditions and how they might arise |
| **Event tree** ***(examines consequences)*** | Graphical representation of possible consequences of an initiating event as well as random effects such as presence of a source of ignition; probabilities assigned to each branch enable the probability of every possible outcome to be determined | To analyse consequences of an incident as part of designing mitigation strategies | Interpret an event tree to understand potential outcomes and effects of a specific event | |
| **Quantitative risk assessment (QRA)** | Mathematical calculation based on a series of assumptions to determine a numerical frequency of a potential event | Used when comparing two or more scenarios to identify the lowest risk option; QRA is often utilised in the preparation of a safety case | Identify and provide relevant information; verify input information; understand underlying assumptions and how they relate to control of work; understand the level of reliability of the outcome, i.e. the results are mathematical approximations | Often supported by modelling software |
| **Layer of protection analysis (LOPA)** | Analytical procedure that draws on fault and event tree analysis to examine the independent protection layers in a plant and the actions should a specific unwanted event occur | Highlights the required system integrity at an early stage of a project; can be used as a quick screening tool to identify the need for a simple or more complex shutdown system; often utilised in preparation of a safety case<br>As assessment and quantification may be subjective, LOPA should be followed up with a fault tree | Be aware of the role and application of LOPA<br>Contribute to discussion on adequacy of level of protection, especially from a qualitative aspect | Typical layers are:<br>• design and engineering<br>• process control system and operating procedures<br>• critical alarms and manual intervention<br>• automatic safety integrity systems and engineering design<br>• physical protection (relief valves) |

| Tool | What is it? | When is it used? | What should an OHS professional do? | Key words / specific knowledge |
|---|---|---|---|---|
| | | where higher levels of integrity are required | | |
| **Safety integrity level (SIL) analysis** | Relative level of risk reduction provided by a safety instrumented function (SIF) expressed as the probability that the safety instrumented system (SIS) will perform its safety function | Used to identify the required integrity of a SIS<br>Often utilised in preparation of a safety case | Be aware of the role and application of SIL | May be determined using tabular methods, LOPA or fault tree analysis<br>Use will depend on:<br>• how often a situation will arise that, if not prevented, will result in a hazardous event<br>• other independent protective systems (layers of protection) and the probability that they will fail on demand to prevent the hazardous event<br>• tolerable frequency of the hazardous consequences |
| **Failure mode and effects analysis (FMEA)** | Takes a selected part of a system, usually a piece of hardware, and examines every failure mode of every item and every element within it; consequences for each failure mode are determined to evaluate the adequacy of the response to the failure | To understand likely failures and common mode failures<br>Used in design, process optimisation and investigation | Be aware of the role and application of FMEA | Often supported by modelling software (FMEA on an engineering item is equivalent to a HAZOP on a process) |
| **Societal risk (FN curve)** | Describes the relationship between the frequency of a scenario and the number of people suffering from a specified level of harm in a given population for a specified hazard; the relationship is often plotted as a cumulative frequency distribution, or FN (frequency-number) curve, giving the frequency of events exceeding a specific stated severity | Typically used for offsite populations, FN curves are often used to show the net risk to people in the event of an incident<br>Used in preparation of a safety case | Identify and provide relevant information | Often supported by modelling software |

# 7 Control

Control of risk to prevent and mitigate hazardous incidents is the overall objective of hazard identification, risk assessment and safety-related management activities for both process safety and OHS professionals. For both professional groups, the priority for control actions is:

- Elimination through design
- Prevention
- Evaluation and assurance
- Mitigation.

Prevention and mitigation are achieved through passive, active and administrative barriers applied within a systematic approach to the process safety and OHS management.

## 7.1 Elimination through design

Inherently safer design (ISD)[24] is based on the premise that it is better to remove the hazard or reduce the magnitude of the hazard than to control it with equipment and procedures. Kletz (1978) summed this up as 'What you don't have can't leak'. The concepts underpinning ISD continue to evolve and increase in importance.

While there are several ways of categorising ISD strategies, the following discussion is based on the five categories identified by IChemE Safety Centre:

- Elimination
- Minimisation/intensification
- Substitution
- Moderation/attenuation
- Simplification (ISC, 2020b)

It is usually not possible to target all hazards in a plant equally. For example, to allow for a reduced inventory of a hazardous chemical, the design may require processing at a higher temperature and pressure; in this case the higher temperature and pressure is accepted to reduce the risk of a hazardous inventory. Another scenario is that there may be two possible

[24] Generalist OHS terminology is likely to refer to 'safe design' or 'engineered safe design'; 'inherently safer design' is more commonly used in process safety to refer to the design of the process.

solvents for a process – one flammable with low toxicity, the other with low flammability but high acute toxicity. The hazard and ISD strategy selected will often represent a compromise based on intensive risk assessment that considers the life cycle of the plant and the technology available at the time.

### 7.1.1 Elimination

Elimination aims to eliminate the hazard completely from the process. This can include removing specific hazardous chemicals from the process, or even eliminating an entire process. Often elimination goes hand in hand with substitution, as one element may be substituted out for a less hazardous option.

### 7.1.2 Minimisation/intensification

Reducing the hazardous energy by reducing the size of the equipment (intensification of the process) is inherently safer as the consequences of a loss of containment will be correspondingly reduced. Use of smaller units also enables implementation of other design safety features such as stronger containment. Process conditions in smaller containers are more uniform so there will be better process control and improved safety. As smaller equipment is cheaper to build there are also financial benefits.

### 7.1.3 Substitution

Substitution of a less-hazardous chemical or process reduces the overall hazards, but must usually be considered at the design stage. Examples of such substitutions are the use of an aqueous solution as a solvent in a purification process rather than a flammable solvent such as toluene or methanol, and cleaning with detergent and water rather than a solvent. Substitution for safety reasons is often linked with strategies to reduce environmental impact of chemicals and chemical processing, also known as sustainable or ‘green’ chemistry (Anastas & Warner, 1998).

### 7.1.4 Moderation/attenuation

Sometimes referred to as attenuation, changing a material or process to moderate a hazard can reduce the consequences of a loss of control. Moderation involves using processes requiring less-hazardous operating conditions, i.e. reaction conditions closer to ambient temperature and atmospheric pressure. This may be achieved by:

- *Dilution* with a less-hazardous material, reducing the impact of a loss of containment and, in some cases, increasing the stability of the chemical
- *Refrigeration* (e.g. storing liquefied natural gas under refrigeration at atmospheric pressure thus reducing the need for pressure containment)

- *Changing physical characteristics* (e.g. handling and transporting a chemical in crystalline form rather than as a fine or combustible dust)
- *Use of a catalyst* to allow a lower operating temperature.

### 7.1.5 Simplification

A complex process or plant is usually more difficult to operate and less tolerant of errors. At the design stage the emphasis should be on the simplest design possible to eliminate a hazard or minimise the need for complex control and safeguard systems. Some general principles are:

- Use of stronger (higher pressure rated) equipment to reduce the need for complex pressure relief systems, instrumentation and interlocks
- Elimination of seldom-used piping
- Processes tolerant to variations in operating parameters and feedstock changes
- Making incorrect operation impossible (e.g. use of selective couplings to prevent inadvertent cross-connection of utilities such as nitrogen and breathing air systems)
- Good human factor design to ensure equipment operates the way people expect it to operate and provides feedback to confirm proper operation (Mannan, 2012).

## 7.2 Prevention

The management environment sets the context in which all aspects of process safety and OHS operate. The management environment can be considered at two levels:

- Organisational 'culture'
- Management systems and processes.

The *OHS Body of Knowledge* chapters 10.1 The Organisation and 10.2 Organisational Culture discuss culture as a concept, noting the generally confusing and ambiguous nature of the literature on organisational culture and safety-related performance. The outcome of discussion in these chapters is that safety is better served by shifting the focus and language from 'safety culture' to organisational and management practices that have a direct impact on risk control in the workplace.[25]

This section considers the components of a systematic approach to managing safety by comparing the process safety and OHS approaches to safety management systems and the

[25] See *OHS BoK* 10.2 Organisational Culture for a review of literature on organisational culture.

specific examples of management of change (MoC) in a process safety environment and safety critical elements (SCEs).[26]

### 7.2.1 Management systems

An OHS management system can be defined as:

> [a] management system or part of a management system used to achieve OHS policy. (ISO/SA/SNZ, 2018, p. 3)

The development of an organisation's system to manage health, safety and the environment draws its inputs from specific work health and safety regulations, standards and the organisation's desire to protect its people, the public and the environment. The role of an organisation's management system is to capture these prescriptive and/or performance-based requirements.

While the elements of a safety management system are usually combined in an integrated OHS management system, the context and focus are different for OHS and process safety. OHS management is aimed at the worker and the hazards inherent in a task or workplace while process safety management is aimed at the plant and the hazards inherent in the process. The focus of process safety is:

- Design integrity management, including the specification and design of plant
- Operational integrity management, which covers the engineering and administrative controls to ensure that assets are operated within their design limitations and safe operating envelopes
- Asset and technical integrity management, which involves inspection and maintenance to ensure that the assumptions and limitations of the plant design are managed throughout the life of the asset and that safety critical controls are assured to meet their defined performance standards.

Appendix 3 compares the elements of ISO/*AS/NZS 45001:2018 Occupational Health and Safety Management Systems – Requirements with Guidance for Use* (SA/SNZ, 2018) with the *Guidelines for Risk Based Process Safety* (CCPS, 2007), highlighting opportunity for integration of the management systems for OHS and process safety to optimise overall safety outcomes.[27]

[26] Readers should also be familiar with *OHS BoK* 12.1 Systems.

[27] Hayes & Zhang (2016) provide an analysis of a range of self-assessment tools and their relevance for assessing the safety management system in a process safety environment.

### 7.2.2 Management of change (MoC)

Poor management of change has been implicated as a causal factor in some process incidents; for example, at Flixborough in 1974 and Bhopal in 1984 (Atherton & Gil, 2008; WorkSafe Victoria, 2020), at BP Grangemouth oil refinery, Scotland, in 1987 (HSE, 1989), and at the Williams Olefins petrochemical plant in Geismar, Louisiana, in 2013 (CSB, 2016).

A process facility has three components:

- *Plant* – the heat exchangers, pipes, pumps, valves, sensors, computers, relief valves, etc., that constitute the hardware and the control software used to operate the facility
- *Process* – the operating conditions (e.g. flow rate, pressure and temperature) required to produce or manufacture the products
- *People* – those who operate the plant and ensure that the process remains within its design limits, those who maintain the plant so it can continue to operate as intended, and those who have accountability over the management of the plant and process.

A facility design is based on certain assumptions (e.g. what is known about the feedstock, the competency of operators), constraints (e.g. how much capital is available to spend on design/construction) and limitations (e.g. physical realities related to materials and resources). These assumptions, constraints and limitations determine the nature of the process, the design and construction of the plant, and the required resources and competencies for operation, maintenance and management of the plant and the process.

The result is typically a bespoke facility with a design that may have limited capacity to adapt to deviations from the design assumptions, constraints and/or limitations. In changing environments, such rigidity may cause the plant, process and/or people to be no longer fit-for-purpose (i.e. no longer able to produce the desired product at the desired rate or quality) or, worse, create an unsafe situation (i.e. a process safety incident). In such cases, the function of safeguards may be compromised or process conditions may exceed the ability of the facility to tolerate them (e.g. pressures/temperatures) and so lead to failure and loss of containment.

Changes are, however, inevitable in most circumstances. For example, changes in feedstock quality or availability, changes in the specifications of products and changes observed in the plant over time will drive a need for the facility to be modified to varying degrees. Changes in production/manufacturing facilities may include both technical changes and organisational changes (WorkSafe Victoria, 2020).

Typical *technical changes* include:

- Changes initiated when legislation, codes of practice or licence conditions are altered or where new requirements are imposed
- Design alternations or alterations to plant, equipment or any hardware (excluding like-for-like changes or replacement-in-kind)
- Alterations to operations (including process parameters, safe operating envelopes set within the pressure/temperature design limits), operating procedures or work instructions
- Changes to software or hardware associated with either process control systems or instrumented protective systems
- Changes to set points initiating instrumented protective systems (e.g. a change to the low-level trip set point for a boiler)
- Materials management (e.g. proposed use of a material that would be new to the facility)
- Changes to inspection, maintenance or testing programs
- Change in site or plant layout
- A series of minor variations or adjustments with a cumulative effect that constitutes a deviation of significance from the original condition (WorkSafe Victoria, 2020).

Typical *organisational changes* include alterations to organisational structure (e.g. additions or deletions of roles) and any changes (permanent or temporary) in the people assigned to:

- Safety critical roles (responsible for assuring the effectiveness of the management system and risk controls)
- Interface with designated internal technical specialists with sign-off authority (often referred to as technical authorities)
- Roles specified in a major hazard facility safety case
- Internal reporting requirements, including key performance indicators
- Interface with government or industry regulators
- Interface with media representatives.

Other types of changes may relate to changes in the asset portfolio, such as the acquisition or divestment of facilities that may result in safety or environmental legacy issues (e.g. contaminated soil, maintenance backlog) that should be considered during a due diligence scrutiny.

Regardless of the activity, where an organisational change can have an impact on the process safety performance and outcomes at a facility, the change must be managed (CCPS, 2013).

For changes to be implemented effectively *and safely*, the potential impacts of the change on all aspects of the facility (or business) should be evaluated, understood and communicated and, where required, the risks mitigated. Most organisations adopt a formal, systematic process for MoC, typically comprising:

- A clear definition of what constitutes a significant change (including changes to the organisation and how temporary modifications are dealt with)
- Consultation with subject matter experts
- Risk assessment of the proposed change
- Designated authority levels for approving the proposed change
- Tracking of the communication and close out of the change
- Identification of any training requirements associated with the change
- Identification of any controlled documents requiring updating.

Formal MoC processes should also ensure that:

- The original scope and duration of all changes (including temporary modifications) are not exceeded without review and formal approval
- Changes are documented (including the rationale and technical basis)
- Temporary changes have a prescribed time limit (not to be exceeded without formal review and approval) (WorkSafe Victoria, 2020).

### 7.2.3 Safety critical elements (SCEs)

The IChemE Safety Centre defines safety critical elements (SCEs) as:

> …a barrier that has been deemed to be critical by the facility or organisation [to ensure the tolerability of the residual risk.] This is usually done on the basis of understanding what consequence the barrier is preventing or mitigating, the likelihood of that consequence happening and the reliability of the barrier. SCEs can be hardware, control system related, or administrative, such as procedures. (ISC, 2015, p. 7)

Compromised design and maintenance of SCEs is a recurring theme in process safety incidents. For example, the report of the investigation into the 2005 Buncefield oil storage incident in the US identified “failure of design and maintenance in both overfill and liquid containment systems” as the technical cause of the initial explosion and the seepage of pollutants to the environment (COMAH, 2011). Reflecting on the Buncefield incident, Joseph (2015) identified the same design failures and observed that reference to international standards for design of SCEs is insufficient to ensure the required level of safer design: “it is vital that appropriate changes to these international standards are made” (p. 29).

In a performance-based legislative regime (section 4) it is a fundamental requirement for facilities to define their own SCEs, and then to implement an assurance regime to ensure they have confidence in the reliability of each element.

Examples of SCEs include:

- Application of a high-quality safe-work or permit-to-work system
- Management of locked/tagged isolation valves
- Activation and operation of automated emergency trip systems that prevent a loss of containment when control is lost (e.g. high-level shutoff on a tank that should fail-to-safe)
- Operation of a pressure relief valve on a pressure vessel at the required conditions
- Injection system to stop a runaway exothermic reaction
- Gas detection equipment
- Fire detection and suppression systems.

In a facility, the process is usually controlled by computer-based systems (e.g. DCS, PLC, SCADA) that manage for operational and quality outcomes, not safety. While these systems can provide indications of safety issues (e.g. alarms), they are generally not safety critical as they lack the independence and reliability usually associated with SCEs. [28]

### 7.2.4 Permit to Work

Permit-to-work (PTW) systems (sometimes called safe systems of work) can illustrate the benefits of collaboration by process safety and OHS professionals. PTW systems are used to evaluate and reduce risks associated with non-routine activities/work in which people intrusively interact with plant and equipment (e.g. to undertake internal vessel inspections or maintenance activities on or near live plant). Such systems require evaluation of potential hazards and implementation of associated controls to protect:

- People from the hazards of the plant (traditionally the concern of OHS professionals)
- Plant from the activities of the people (usually the purview of process safety professionals).

Where these two objectives are considered and addressed separately there is a potential for incomplete coverage of the hazards and risk, or a conflict that may actually increase the risk.

Controls implemented as part of the PTW process may relate specifically to managing occupational risks (e.g. breathing apparatus for entering confined spaces and harnesses for working at heights). However, an integrated approach to PTW as an outcome of a joint understanding of the objectives and constraints of both process safety and OHS will optimise both the risk management and operational outcomes (Table 7).

[28] For further information on SCEs refer to IOGP, (2016) Standardization of barrier definitions. Supplement to Report 415.

**Table 7: Example outcomes of an integrated, collaborative approach to PTW**

| Control | Process safety aspects | Occupational safety aspects |
|---|---|---|
| Control of critical lifts | Prevents a large loss of containment when lifting loads over live plant | Prevents injuries when lifting loads over work areas within a plant |
| Control of simultaneous operations | Prevents unplanned interaction of tools/equipment/work with plant | Prevents unintended interaction of tools/equipment/work with people |
| Positive isolation of live process streams | Prevents a loss of containment when workers open the plant to atmosphere | Prevents exposure to hazardous chemicals and energy during the work activities |
| Gas detection and ignition control | Detects the presence of a small leak enabling prevention of ignition and escalation to nearby plant | Prevents illness and/or injury from toxic gas or ignition of flammable gas by 'hot' work |

## 7.3 Evaluation and assurance

Assurance that safety systems are in place and working as intended is vital. Deficiencies in the monitoring of safety and hazard management systems have been implicated in several process safety disasters. A focus on lost time injuries (LTIs) and relatively minor matters is considered a causal factor in both the 1994 Moura mine disaster in central Queensland and the 1998 Longford gas plant explosion (Hopkins, 2000). A failure to learn about the need for valid and reliable performance measures was identified in the Texas City refinery disaster and the Gulf of Mexico Macondo well blowout (Hopkins, 2012).

Auditing, as an assurance activity, comes under similar criticisms. Shortcomings in either audit processes or responses to audits have been implicated in incidents, including those at Piper Alpha, Longford, Texas City and Macondo (Hopkins, 2000, 2008, 2012).

### 7.3.1 Performance indicators

Valid and reliable health and safety performance measures relevant to the situation and the process are essential for evaluating the effectiveness of strategies for managing both OHS and process safety.

The definition of performance measures for OHS is a topic of some discussion among OHS professionals. The historical use of LTIs and the more encompassing 'total injuries' has come under criticism (O'Neill, Martinov-Bennie, Cheung & Wolfe, 2013). While there has

been a move away from injury outcome measures in favour of positive (or leading) performance indicators, such measures are also seen to have significant problems, not least of which is the tendency for people and organisations to 'manage the measure rather than the performance'. The definition of effective safety performance measures remains hotly contested (O'Neill et al., 2013).[29]

Process safety has suffered from a similar lack of agreed performance measures that address lag and lead indicators that are practical to implement. This chapter takes the position that both lead and lag measures are important in evaluating safety performance, and draws attention to lag metrics described by the American Petroleum Institute (API, 2021a) and lead indicators developed by the IChemE Safety Centre (ISC, 2015).

The API (2021a) defines process safety indicators in terms of tiers. The count of Tier 1 process safety events is the most lagging performance indicator and represents incidents with greater consequence resulting from actual losses of containment. The count of Tier 2 process safety events represents loss of primary containment events with a lesser consequence, but may be predictive of future, more significant incidents.

Any Tier 1 or Tier 2 Process Safety Event begins with an unplanned or uncontrolled release of any material, including non-toxic and non-flammable materials from a process that results in one or more consequences described in the RP. (API, 2021b)

Leading indicators for process safety (Table 8) were developed by the IChemE Safety Centre as a result of extensive industry consultation mediated by a technical panel.

[29] OHS performance evaluation is a planned future topic for the *OHS BoK*.

**Table 8: Process safety leading metrics (ISC, 2015, p. 8)**

| Elements | Metrics |
|---|---|
| Knowledge & competence | Conformance with process safety related role competency requirements |
| Engineering & design | Deviations to safety critical elements (SCEs)<br>Short-term deviation to SCE<br>Open management of change on SCEs<br>Demand on SCE<br>Barriers failing on demand |
| Systems & procedures | SCE inspections performed versus planned<br>Barriers failing on test<br>Damage to primary containment detected on test/inspection<br>SCE maintenance deferrals (approved corrective maintenance deferrals following risk assessment)<br>Temporary operating procedures (TOPs) open<br>Permit-to-work checks performed according to plan<br>Permit-to-work non-conformance<br>Number of process safety related emergency response drills to plan |
| Assurance | Number of process safety related audits to plan<br>Number of non-conformances found in process safety audits |
| Human factors | Compliance with critical procedures by observation<br>Critical alarms per operator hour (EEMUA, 1999)<br>Standing alarms (EEMUA, 1999) |
| Culture | Open process safety items<br>Number of process safety interactions that occur |

### 7.3.2 Assurance

Assurance, usually through auditing, is a key aspect in both OHS and process safety and is vital in assisting company officers to meet due diligence requirements. [30]

Assurance is explained by the IChemE Safety Centre as a

> …program for the systematic monitoring and evaluation of all aspects of a business. This includes tools such as auditing, inspection, testing, monitoring, verification and audit. This also applies to defining performance standards and metrics for an organization and reporting performance against them, in addition to the feedback loop, resulting in actions based on data. (ISC, 2024)

[30] *OHS BoK* 9.2 WHS Law in Australia discusses due diligence. The IChemE Safety Centre offers a program targeted at officers of corporations to help them understand their obligations for due diligence as it applies to process safety.

Assurance requires the provision of proof regarding the good 'health' of the safety management system and presumes that without such proof a system is failing. Seeking ‘reassurance’ rather than requiring proof results in a false sense of the status of the systems that may not identify warning signals of future failure. Such false confidence may also allow the removal of operating barriers that would otherwise mitigate the consequences. For example, when SCEs are defined in a safety case they must be monitored against established performance standards to provide assurance that they exist, are maintained and have the required reliability as claimed in the safety case. When the performance varies from the defined standard, the impact of the deviation on the overall risk must be understood and the deviation investigated to understand why and what needs to be done to bring performance back into line.

Audit is defined in *ISO 45001:2018* Occupational health and safety management systems – Requirements with guidance for use (ISO, 2018) as:

> Systematic, independent and documented process for obtaining audit evidence and evaluating objectively to determine the extent to which the audit criteria are fulfilled. (p. 7)

This definition is circuitous and makes no reference to the role of an audit in assessing the adequacy or effectiveness of the OHS management processes overall.

Process safety and OHS audits differ in the focus of the audits with process safety focusing on technical aspects and OHS on management system elements. They both require in-depth examination of valid and reliable evidence (often an area of concern) and the outcomes of both can be optimised by collaboration and sharing information across process safety and OHS audits.

## 7.4 Mitigation

The *OHS Body of Knowledge* chapter, 36 Emergency Management examines key concepts in emergency preparedness for organisations. Emergency plans are an essential part of the total emergency planning framework. Facility plans need to be compatible and integrated with relevant statutory emergency management arrangements, such as local emergency management committees. Where there are concentrations of hazardous facilities in an area, incident and area-specific plans are also needed. In addition, emergency service agencies have their own plans and procedures for responding to incidents and emergencies.

Safe Work Australia has developed detailed guidance for emergency planning for major hazard facilities with emphasis on emergency planning as a systematic process requiring careful planning “based on an appreciation and understanding of the possible emergency scenarios, their possible impacts and the availability of emergency response resources both

internal and external to the facility" (SWA, 2012, p. 8). This planning process is summarised in Figure 7. While the guide is written for MHFs, it provides a useful basis for emergency planning for any facility with process hazards.

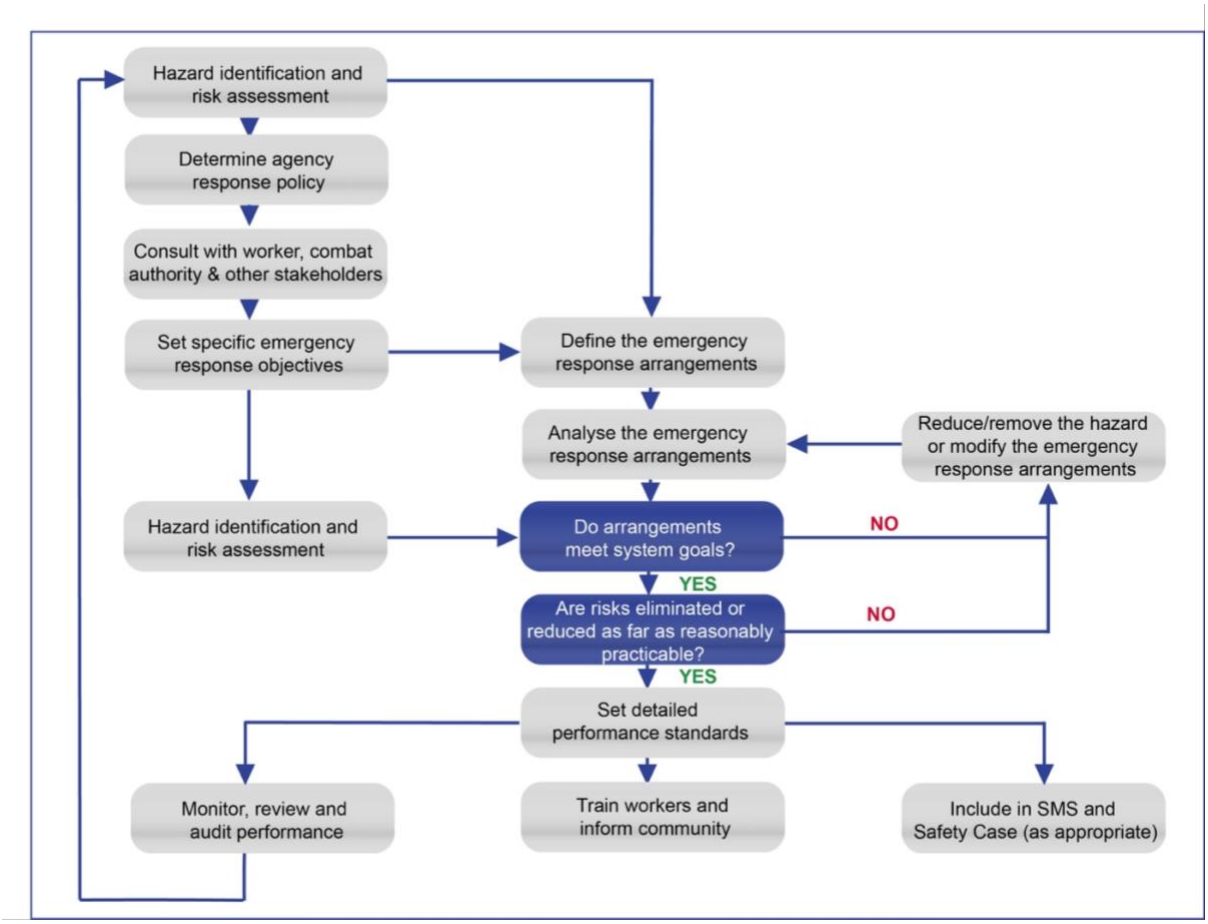



**Figure 7: Emergency planning preparation (SWA, 2012, p.8)**

Emergency plans for major hazard facilities must meet requirements specified in legislation.

> The operator of a determined MHF must prepare an emergency plan for the facility that:
> - addresses all health and safety consequences of a major incident occurring [especially any offsite impacts]
> - includes all matters specified in [the regulation applicable to the organisation
> - provides for testing of emergency procedures, including the frequency [and nature] of testing.
>
> The operator must keep a copy of the emergency plan at the facility and must consult the workers [and other stakeholders] when preparing the emergency plan. (SWA, 2012, p. 3)

The plan must include:

- *Site hazard and details* including location of the facility, site map (covering site, surroundings, hazardous chemical storage), inventory of all hazardous chemicals present, brief description of nature of the facility, emergency response plan and any assumptions
- *Command structure and site personnel* to be activated in the event of emergency – their details, emails and mobile phone numbers
- *Notifications* – the procedures that enable the facility operator to notify emergency services for help and to inform local community and authorities of information about the event, both during and post-event
- *Resources and equipment* available onsite and offsite, including personal protective equipment, gas detectors, wind velocity detectors and decontamination equipment, and procedures to obtain additional help from external agencies where required
- *Procedures* for safe evacuations, decontamination, control of any incident involving hazardous substances controlled through legislation (SWA, 2012).

# 8 Implications for OHS practice

As described in section 1.3, process safety differs from OHS in terms of:

- Mechanisms of causation
- Scale of the potential consequences
- Focus on engineering and design.

Two key factors in the causation of process safety incidents have been identified as:

- A failure to distinguish the need for different approaches to managing hazards associated with low-likelihood, high-consequence incidents
- Assumptions that strategies for managing personal safety would similarly create safe conditions in process safety, and that metrics used to monitor personal safety also provide information on the status of process safety.

Process hazards have traditionally been managed by those with engineering expertise who have good technical knowledge, but may not understand or appreciate the broader context of OHS and the organisational structures and culture within which process safety and OHS operate. Also, generalist OHS professionals may not understand the nature of process hazards, the magnitude of the consequences, nor the technical risk management and control processes routinely employed in process safety. Indeed, the chapter has identified that process safety and OHS professionals often operate in silos.

However, the chapter has also identified significant overlap between the management of process safety and personal safety, and the roles of process safety and OHS professionals. This overlap provides opportunity to optimise both process safety and OHS. Thus, rather than isolating process safety and OHS there should be greater collaboration between the two disciplines.

As the custodian for safety management systems within the organisation and for local-level facilities, the generalist OHS professional requires knowledge of the formal processes for managing process safety and to facilitate the integration of process safety within the formal safety management system. Generalist OHS professionals should ensure that process safety resources and organisational capability exist and, where applicable, are developed and enhanced to enable organisations to become increasingly informed and build broad risk intelligence related to their operations. Similarly, process safety professionals should support the engagement of OHS professionals in process safety activities.

Additionally, there is significant overlap between process safety and OHS professional roles that can be better leveraged to ensure improved management of both process safety and OHS risk (e.g. risk assessment and auditing).

Collaboration between process safety and OHS professionals will require a change in practice by professionals from both disciplines, who will need to recognise and value their commonalities and potential synergies as well as their specialist expertise. This chapter provides a knowledge base to facilitate such engagement by the generalist OHS professional with some specific recommendations for practice outlined below.

*Knowledge development*

- Review *OHS Body of Knowledge* chapters Process Hazards (Chemical) and Managing Process Safety to identify if you are likely to encounter such hazards in your OHS practice and what you might learn from the chapters to inform your practice (even if currently you do not encounter process hazards)
- Clarify your role in managing process hazards at your site/organisation
- Identify if you require further knowledge not addressed in this chapter (and seek a mentor and/or review the Useful Resources section).

*Engagement*

- Take the initiative in learning more about the process hazards in your organisation (see comment about ‘walking the lines’ in section 6.1)
- Seek a process safety professional mentor as a way of increasing your knowledge and facilitating wider engagement; where there is no process safety professional on site or in the organisation seek other networking opportunities to develop contacts
- Initiate discussions about the comparative roles of OHS professionals and process safety professionals and the benefits of collaboration in your organisation (Use

comparative examples in this chapter as a starting point for discussion; there may be different views from those in the documented examples that will support discussion leading to a shared understanding.)

- Promote a collaborative and joint approach to auditing and the emergency preparedness
- Where there is no process safety professional on site or in the organisation, identify the gaps in your knowledge and indicators, and ensure you know when to call in a specialist; engage with operational personnel and others to ensure you are sufficiently familiar with the task and the hazards to assist in developing the scope and brief for any consultant support
- Ensure the OHS function and perspective are considered in risk assessments and business cases related to process safety
- Apply process safety principles and tools as appropriate to enhance OHS practice.

# 9 Summary

Process safety is about preventing incidents that, whilst having a low likelihood of occurrence, are associated with disastrous potential consequences that may include loss of life and serious injury, severe environmental impact, and substantial financial and business reputation losses. In some jurisdictions, process safety is often associated with major hazard facilities, which come under specific legislation. However, such hazards and the associated risks should not be seen to be limited to sites classified as MHFs as this excludes many high-risk situations.

Key factors in process safety incidents have included failure to distinguish the need for different approaches to managing process hazards compared with OHS, and the incorrect assumptions that strategies for managing OHS also create safe conditions in process safety and that metrics used to monitor OHS also provide information on the status of process safety. While there may be some contributory features common to process safety and OHS incidents, the causation mechanisms are different.

Process safety and OHS professionals approach hazard identification and risk assessment from different perspectives. Process safety professionals focus on the operational risks associated with process equipment, usually using data-driven, analytical semi-quantitative and quantitative risk assessment tools to inform the development of engineered controls. In comparison, OHS professionals focus on risks associated with the work undertaken by people, with hazard identification and risk assessment usually featuring a combination of qualitative and semi-quantitative methods informed by data from a range of sources, including consultation with those impacted by the risk. This analysis informs controls that take account of all the components of the sociotechnical system as represented by work in an organisational environment comprising people.

Process safety risk management occurs within a systematic management approach that includes a safety management system, formal processes for managing change and assurance processes to ensure reliability of safety critical systems. In process safety, the priorities for control focus on safer design with the emphasis being on ‘loss of control’ as a precursor to a potential loss of containment.

Management of process safety will achieve better outcomes where there is an integrated approach. Typically, such an approach will be led by the process safety professional who recognises, values and facilitates the contribution of the OHS professional. Effective engagement of the OHS professional in process safety requires an understanding of the concepts outlined in this chapter.

# Useful resources

SWA (Safe Work Australia), Major Hazard Facilities (MHF)
https://www.safeworkaustralia.gov.au/safety-topic/industry-and-business/major-hazard-facilities

HSE (Health and Safety Executive), UK. Control of Major Hazards (COMAH)
http://www.hse.gov.uk/comah/

Institution of Chemical Engineers (IChemE) training programs
https://www.icheme.org/training-events/training/process-safety-courses/

CCPS (Center for Chemical Process Safety, USA https://www.aiche.org/ccps

AIHS online training programs
https://www.aihs.org.au/Web/Web/Learning_and_Events/Online-Courses.aspx?hkey=b639b3b7-1bab-4240-b1bf-f2aec4a0a6d9

# References


AAP (Australian Associated Press). (2011, December 6). Part of Orica plant to be reopened. *Sydney Morning Herald.* Retrieved from http://www.smh.com.au//breaking-news-national/part-of-orica-plant-to-be-reopened-20111206-1ogk1.html

ABC. (2011, December 8). Residents anger over latest Orica leak. *ABC News.* Retrieved from http://www.abc.net.au/news/2011-12-08/residents-anger-over-latest-orica-leak/3719196

ABC. (2013, October 2). Cootes trucks taken off the road after fatal tanker explosion in Mona Vale. *ABC News.* Retrieved from http://www.abc.net.au/news/2013-10-02/mechanical-failure-suspected-cause-of-tanker-explosion/4994502

ABC. (2016, February 19). Cootes crash driver Shane Anthony Day found not guilty. *ABC News.* Retrieved from http://www.abc.net.au/news/2016-02-19/cootes-crash-driver-shane-anthony-day-found-not-guilty/7184762

ABC. (2018, September 25). Longford gas plant workers remembered 20 years pm from deadly explosion. *ABC News*. Retrieved from https://www.abc.net.au/news/2018-09-25/20-years-since-deadly-longford-gas-plant-explosion/10299988

AIHA (American Industrial Hygiene Association). (2016). *Emergency Response Planning Guidelines*. Retrieved from https://www.aiha.org/get-involved/AIHAGuidelineFoundation/EmergencyResponsePlanningGuidelines/Pages/default.aspx

Anastas, P. T. & Warner, J. C. (1998). *Green chemistry: Theory and practice*. New York: Oxford University Press.

API (American Petroleum Institute). (2021a). *Recommended Practice 754 Process Safety Performance Indicators for the Refining and Petrochemical Industries 3e*. Washington DC: API Publishing.

API (American Petroleum Institute). (2021b). *Fact Sheet*: *Recommended Practice 754 Process Safety Indicators for the Refining and Petrochemical Industries*. Washington DC: API Publishing.

Atherton, J. & Gil, F. (2008). *Incidents that define process safety*. New Jersey: John Wiley & Sons Inc.

Broughton, E. (2005). The Bhopal disaster and its aftermath: A review. *Environmental Health*, *4*(1), 6.

Burdeau, C. (2016, July 14). BP estimates cost of 2010 Gulf oil spill at $61.6 billion. *AP News.* Retrieved from https://apnews.com/15247c9394684b86baf0fff7fa2489c7

CCPS (Center for Chemical Process Safety, American Institute of Chemical Engineers). (2007). *Guidelines for risk based process safety*. Hoboken, NJ: Wiley.

CCPS (Center for Chemical Process Safety, American Institute of Chemical Engineers). (2009). *Inherently safer chemical processes: A life cycle approach* (2nd ed.). Hoboken, NJ: Wiley.

CCPS (Center for Chemical Process Safety, American Institute of Chemical Engineers). (2010). *Guidelines for process safety metrics.* New York, NY: Wiley.

CCPS (Center for Chemical Process Safety, American Institute of Chemical Engineers). (2013). *Guidelines for Managing Process Safety Risks During Organizational Change.* New York, NY: Wiley.

CCPS (Center for Chemical Process Safety, American Institute of Chemical Engineers). (2017). *Process Equipment Reliability Database (PERD)*. https://www.aiche.org/ccps/resources/process-equipment-reliability-database-perd

COMAH (Control of Major Accident Hazards). (2011). *Buncefield: Why Did It Happen?* HSE. Retrieved from https://webarchive.nationalarchives.gov.uk/ukgwa/20220701154114/https://www.hse.gov.uk/comah/buncefield/index.htm

Cooper, A. (2014, October 8). Cootes Transport fined more than $50,000 for unsafe tankers following fatal crash. *The Age.* Retrieved from http://www.theage.com.au/victoria/cootes-transport-fined-more-than-50000-for-unsafe-tankers-following-fatal-crash-20141008-10rq0d.html

CSA Group (Canadian Standards Association). (2022). *Process safety management*. Toronto: CSA Group

CSB (US Chemical Safety and Hazard Investigation Board). (2016). *Williams Geismar Olefins Plant: Reboiler Rupture and Fire, Geisma, Louisiana* (Case Study). Washington, DC: CSB. Retrieved from https://www.csb.gov/williams-olefins-plant-explosion-and-fire-/

Cullen, W. D. (1990). *The public inquiry into the Piper Alpha disaster* (Vols I & II). London: HMSO.

da Cruz, M. & Bentes, S. R. (2013). The Seveso directives and their application to enterprise risk management. *International Journal of Latest Trends in Finance & Economic Sciences*, *3*(3), 563-571.

Dekker, S. (2006). *The field guide to understanding human error*. Aldershot, England: Ashgate.

EC (European Commission). (2015). Industrial accidents: The Seveso Directive – Prevention, preparedness and response. Retrieved from http://ec.europa.eu/environment/seveso/

EI (Energy Institute). (2022). *High level framework for process safety management*. London: EI

Exida. (2015). *Safety equipment reliability handbook* (4th ed.). http://www.exida.com/Books/Safety-Equipment-Reliability-Handbook-4th-Edition

Hackitt, DJ. Taking the Blinkers Off. Paper presented at : Thomas Ashton Lecture, 2022. Retrieved from https://documents.manchester.ac.uk/display.aspx?DocID=60822

Hayes, J., & Zhang, R. (2016). Process Safety self-assessment tools: What is out there and what do they mean for your organisation? *J. Health, Safety and Environment*. Vol: 32(3), pp.169-186.

Hendershot, D. C. (2009). A history of process safety and loss prevention in the American Institute of Chemical Engineers. *Process Safety Progress, 28*(2), 105-113.

Hopkins, A. (1999). Repeat Disasters: The Lessons of the Moura Coal Mine. In C. Mayhew & C. L. Peterson (Eds.), *Occupational health and safety in Australia*. Sydney, NSW: Allen and Unwin.

Hopkins, A. (2000). *Lessons from Longford: The Esso gas plant explosion*. Sydney, NSW: CCH Australia Ltd.

Hopkins, A. (2005). *Preventing disaster: Learning from Longford* [video]. Sydney, NSW: Futuremedia.

Hopkins, A. (2008). *Failure to learn: The BP Texas City refinery disaster*. Sydney, NSW: CCH Australia Ltd.

Hopkins, A. (2012). *Disastrous decisions: The human and organisational causes of the Gulf of Mexico blowout*. Sydney, NSW: CCH Australia Ltd.

HSE (Health & Safety Executive, UK). (1989). *The Fires and Explosions at BP Oil (Grangemouth) Refinery Ltd*. London: HSE.

IChemE (Institution of Chemical Engineers). (2016). Hazard Identification Techniques [training course]. Rugby, UK: IChemE.

ILO (International Labour Organisation). (2006). Chernobyl 20 years after: From disaster, breeding a new safety culture. Retrieved from https://www.ilo.org/resource/article/chernobyl-20-years-after-disaster-breeding-new-safety-culture

IOGP (International Association of Oil & Gas Producers). (2016). *Standardization of Barrier Definitions: Supplement to Report 415* (Report 544). England: IOGP.

ISC (IChemE Safety Centre). (2024). *Process Safety Framework*. Retrieved from https://www.icheme.org/knowledge-networks/safety-centre/framework/

ISC (IChemE Safety Centre). (2015). *Lead Process Safety Metrics – Selecting, Tracking and Learning.* Retrieved from https://www.icheme.org/knowledge-networks/safety-centre/publications/assurance/

ISC (IChemE Safety Centre). (2018). *Process Safety Competency – A Model*. Retrieved from https://www.icheme.org/knowledge-networks/safety-centre/publications/knowledge-and-competence/

ISC (IChemE Safety Centre). (2020a). *Process Safety Competency Supplementary guide – how to build and develop process safety competence.* Retrieved from https://www.icheme.org/knowledge-networks/safety-centre/publications/knowledge-and-competence/

ISC (IChemE Safety Centre). (2020b). *Applying process safety during concept select phase of a project.* Retrieved from https://www.icheme.org/media/24990/lc-0066_23-applying-ps-during-concept-disclaimer-addition.pdf

Joseph, M. (2015). Buncefield: A decade on. *Chemical Engineer*, *894/895*, 26-29. Retrieved from https://www.thechemicalengineer.com/features/buncefield-a-decade-on/

Kerin, T. (2015). The evolution of process safety standards and legislation following landmark events—what have we learnt? *Process Safety Progress, 35*(2), 165-170.

Kletz, T. (1978). What you don't have can't leak. *Chemistry & Industry, 6*, 287-292.

Kletz, T. (1985). *What went wrong? Case histories of process plant disasters and how they could be avoided* (5th ed.). Oxford/Rugby, UK: Butterworth-Heinemann/IChemE.

Kletz, T. (1993). *Lessons from disaster: How organisations have no memory and accidents recur.* Warwickshire: IChemE.

Kletz, T. (2001). *An engineer's view of human error* (3rd ed.). Warwickshire: IChemE.

Kletz, T. (2003). *Still going wrong! Case histories of process plant disasters and how they could have been avoided*. Burlington, MA: Butterworth-Heinemann.

Mannan, S. (Ed.). (2012). *Lee's loss prevention in the process industries* (4th ed.). Oxford: Butterworth-Heinemann.

Marsh. (2022). *100 largest losses in the hydrocarbons Industry 1974-2021* (27th ed.). London: Marsh & McLennan.

McAleese Group. (2014, June 4). ASX Announcement. Retrieved from https://announcements.asx.com.au/asxpdf/20140604/pdf/42q0nby7b25mjg.pdf

Nicol, J. (2001). *Have Australia's Major Hazard Facilities Learnt from the Longford Disaster? An Evaluation of the Impact of the 1998 Esso Longford Explosion on Major Hazard Facilities in 2001.* Institution of Engineers, Australia. Retrieved from https://www.adepp.com/files/Longford_incidentinvestigation.pdf

NOPSEMA (National Offshore Petroleum Safety and Environmental Management Authority). (2022). *The Safety Case in Context: An Overview of the Safety Case Regime* (Guidance Note). Retrieved from https://www.nopsema.gov.au/sites/default/files/documents/The%20safety%20case%20in%20context%20An%20overview%20of%20the%20safety%20case%20regime.pdf
NOPSEMA (National Offshore Petroleum Safety and Environmental Management Authority. (2019). *Introducing NOPSEMA*. Retrieved from https://www.nopsema.gov.au/assets/Publications/A631330.pdf

NRDC (Natural Resources Defence Council). (2015). *Summary of Information Concerning the Ecological and Economic Impacts of the BP Deepwater Horizon Oil Spill Disaster* (NRDC Issue Paper). New York. Retrieved from https://www.nrdc.org/sites/default/files/gulfspill-impacts-summary-IP.pdf

NSW Parliament. (2012). *Select Committee on the Kooragang Island Orica Chemical Leak.* Sydney, NSW: NSW Parliament, Legislative Council.

NSW Department of Planning. (2011). *Safety Management* (Hazardous Industry Planning Advisory Paper No. 9). Retrieved from https://www.planning.nsw.gov.au/sites/default/files/2023-03/hazardous-industry-planning-advisory-paper-no-9-safety-management.pdf

NYSE (New York Stock Exchange). (2016). BP P.L.C. (XNYS:BP): Quote data. Retrieved from https://www.nyse.com/quote/XNYS:BP

O'Neill, S., Martinov-Bennie, N., Cheung, A., & Wolfe, S. (2013). *Issues in the Measurement and Reporting of Work Health and Safety Performance: A Review.* NSW: Macquarie University.

O'Reilly, B. (2011). *A Review into the Response to the Serious Pollution Incident at Orica Australia Pty. Ltd. Ammonium Nitrate Plant at Walsh Point, Kooragang Island on August 8 2011.* NSW Department of Premier and Cabinet. Retrieved from

https://www.nsw.gov.au/sites/default/files/2023-07/A-review-into-the-response-to-the-serious-pollution-incident-at-Orica-Australia-Pty-Ltd-plant-Walsh-Point.pdf

OSHA (Occupational Safety and Health Administration). (2000). *29CFR 1910.119 Process Safety Management of Highly Hazardous Chemicals*. US Department of Labor. https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9760

Reason, J. (1997). *Managing the risks of organizational accidents.* Aldershot: Ashgate.

Robens, A. (1972). *Safety and Health at Work* (Report of the Committee 1970-1972). London: HMSO.

SA/SNZ (Standards Australia/Standards/Standards New Zealand. (2018). ISO 45001: 2018 *Occupational Health and Safety Management Systems – Requirements with Guidance for Use*. Sydney and Wellington: Standards Australia/Standards New Zealand

Sikora, K. (2011, November 10). Orica's Kooragang Island plant shut down. *Daily Telegraph.* Retrieved from http://www.dailytelegraph.com.au/oricas-stockton-plant-shut-down/news-story/fbffc74d64db177837da0c8058345223

SWA (Safe Work Australia). (2023a). *Australian Work Health and Safety Strategy 2023-2033.* Canberra, ACT: Safe Work Australia. Retrieved from https://www.safeworkaustralia.gov.au/sites/default/files/2023-10/australian_whs_strategy_2023-33_october2023.pdf

SWA (Safe Work Australia). (2012*). Guide for Major Hazard Facilities – Emergency Plans*. Canberra, ACT: Safe Work Australia. Retrieved from https://www.safeworkaustralia.gov.au/doc/guide-major-hazard-facilities-emergency-plans

SWA (Safe Work Australia). (2023b). Model Work Health and Safety Act . Canberra, ACT: Safe Work Australia. Retrieved from https://www.safeworkaustralia.gov.au/sites/default/files/2023-12/model-whs-bill-23_november_2023.pdf

The Age. (2004, November 9). $32m gas blast compo for business. *The Age*. Retrieved from https://www.theage.com.au/national/32m-gas-blast-compo-for-business-20041109-gdyyfi.html

UN (United Nations). (2017). *Globally Harmonized System of Classification and Labelling of Chemicals (GHS)* (7th ed.). New York and Geneva: United Nations. Retrieved from https://unece.org/ghs-rev7-2017

Viner, D. (2015). *Occupational risk control: Predicting and preventing the unwanted.* Surry: Gower.

Whitford, D. Burke, D., & Elkind, P. (2011, January 25). BP: 'An accident waiting to happen.' *Fortune.* Retrieved from http://fortune.com/2011/01/24/bp-an-accident-waiting-to-happen/

Wiggins, J. (2014, August 27). McAleese delivers loss after Cootes tanker crash. *Australian Financial Review.* Retrieved from http://www.afr.com/business/transport/trucking/mcaleese-delivers-loss-after-cootes-tanker-crash-20140826-jczab

Wiggins, J. (2016a, March 16). McAleese future hangs on financial restructure after $97m net loss. *Australian Financial Review.* Retrieved from https://www.afr.com/markets/equity-markets/mcaleese-future-hangs-on-financial-restructure-after-97m-net-loss-20160316-gnkccw

Wiggins, J. (2016b, August 29). McAleese collapses as recapitalisation plan falls apart. *Australian Financial Review.* Retrieved from http://www.afr.com/business/mcaleese-collapses-as-recapitalisation-plan-falls-apart-20160828-gr3agn

WorkSafe Victoria. (2020). *Management of Change at a Major Hazard Facility* (Guidance Note). Retrieved from https://www.worksafe.vic.gov.au/resources/management-change-major-hazard-facility

WorkSafe Victoria. (2012-24). Prosecution result summaries & enforceable undertakings. Retrieved from https://www.worksafe.vic.gov.au/prosecution-result-summaries-enforceable-undertakings

# Appendix 1: Common acronyms used in process safety

| | | | |
|---|---|---|---|
| ALARP | As low as reasonably practicable | LOP | layer of protection |
| API (RP) | American Petroleum Institute (Recommended Practice) | LOPA | layer of protection analysis |
| ASTM | American Society for Testing and Materials | LOPC | loss of primary containment |
| ATEX | atmosphères explosibles (European explosive atmosphere standard) | MAOP | maximum allowable operating pressure |
| BLEVE | boiling liquid expanding vapour explosion | MoC | management of change |
| BOP | blowout preventer | PES | programmable electronic systems |
| BPCS | basic process control system | P&ID | piping and instrumentation diagram |
| CHAZOP | control hazard and operability study | PFD[31] | probability of failure on demand |
| DCS | distributed control system | PFD | process flow diagram |
| E&I | electrical and instrumentation | PLC | programmable logic controller |
| ENVID | environmental impact identification | PFH | probability of failure per hour |
| ELD | engineering line diagram | PHA | process hazard analysis |
| ER | emergency response | PRD | pressure relief device |
| ERA | environmental risk assessment | PRV | pressure relief valve |
| ERPG | emergency response planning guidelines | PSFS | process safety flow schematic |
| ESD | emergency shutdown | PS MS | process safety management system |
| FEED | front-end engineering design | PSE | process safety event |
| FMEA | failure mode and effects analysis | PTW | permit to work |
| FMECA | failure mode, effects and criticality analysis | QRA | quantitative risk assessment |
| FN | cumulative frequency (F) of number (N) fatalities | SCADA | supervisory control and data acquisition |
| FTA | fault tree analysis | SCE | safety critical element |
| HAZID | hazard identification study | SIF | safety instrumented function |
| HAZOP | hazard and operability study | SIMOPS | simultaneous operations |
| HF | human factors | SIS | safety instrumented system |
| HIPPS | high integrity pressure protection system | SQRA | semi-quantitative risk assessment |
| HLA | high-level alarm | SR | societal risk |
| HLSD | high-level shutdown | SRS | safety requirements specification |
| IR | individual risk | TEL | threshold exposure limit |
| IRPA | individual risk per annum | TLV | threshold limit value |
| kPa | kilopascal (unit of measure for pressure) | TWA | time-weighted average |
| LEL | lower explosive limit | UEL | upper explosive limit (same as UFL) |
| LFL | lower flammable limit | UFL | upper flammable limit (same as UEL) |
| LOC | loss of containment | UPS | uninterruptible power system |

[31] The acronym PFD occurs twice; the use of this acronym in process safety is context specific.

# Appendix 2: Comparative role and interface of process safety and generalist OHS professionals – scenario of an LPG tanker[32]

| | | Process Safety specialist | Overlap | Generalist OHS professional |
|---|---|---|---|---|
| **Knowledge & competence** | Process safety concepts | The whole system, but with focus on site and driver | Public and environmental impact | Driver safety |
| | Hazard identification & risk assessment | | Hazard identification and risk assessment with some different areas of focus as well as overlap<br>Route-specific issues | |
| | Hazard awareness & characterisation associated with the system being operated and the product processed | | Hazmat signage<br>Product awareness | Licensed and competent drivers, including Hazmat |
| **Engineering & design** | Safety in design, including systems | Integrity of tank and delivery hoses, excess flow valves, sheer points of equipment, pressure relief, tanker overfill safeguard, electrical immobilisation, interlocks, earthing integrity during load transfer | Truck chassis design, load capacity, crash protection; site design; deluge cage design<br>Shared understanding of requirements to ensure 'fit for purpose' design | Driver access to cab; posture issues in cab seating; weight and manoeuvrability of delivery hoses<br>Dashboard design |
| | Asset integrity – inspection & maintenance | Inspection and maintenance of SCEs | Roadworthy and vehicle maintenance | Competency, supervision, fitness for work of vehicle maintenance workers |

[32] As the respective roles will vary depending on the way they are viewed and managed in an organisation and based on the background of the individual, this table is not intended to be complete or definitive, but is provided for illustration and discussion.

| | | Process Safety specialist | Overlap | Generalist OHS professional |
|---|---|---|---|---|
| | | | Supervision and competence of gas fitting maintenance workers | |
| | Management of change | MoC of SCEs | MoC to design, processes and procedures | MoC in design, scheduling, rostering, driver competency |
| | Codes and standards | Pressure equipment codes | Design codes | Fatigue management codes |
| **Systems & procedures** | Safe systems of work | Manage and monitor performance of SCEs | Awareness of range and role of controls for process and OHS hazards and how the controls may impact other aspects of operations<br><br>Control of maintenance work | Manage implementation of controls and monitor effectiveness |
| | Systems, manuals & drawings | Design, interpret and modify P&IDs for tanker and loading system | As part of a multidisciplinary team, use P&IDs to evaluate risk and effectiveness of controls | Read and interpret P&IDs for tanker and loading system |

| | | Process Safety specialist | Overlap | Generalist OHS professional |
|---|---|---|---|---|
| | Process & operational status monitoring and handover | Records on tanker levels and pumping rates<br>Load transfer issues onsite<br>Location of loading bay bunds, mounded bullets, ground slopes (spill handling)<br>Transfer procedures and responsibilities<br>Potential for incorrect contents for storage, liquid and vapour transfer process<br>Complex piping connections to multiple storage<br>Odourisation requirements,<br>Thermal pressure relief<br>Correct hoses and couplings for transfer requirements<br>Potential failure modes<br>Monitoring processes for SCEs | Operating envelopes<br>Static electricity discharge<br>Management of ignition sources<br>Tanker interaction with plant trips and safeguards<br>Gas detection, hazardous area classification<br>Tanker routing, roads within site, traffic management plan<br>Driver responsibilities onsite especially unmanned transfer procedures<br>Minimum load transfer requirements for different sites<br>Drive-away protection, key handling<br>Driver interaction with the public and operators, establishment of exclusion zones during delivery<br>Implications of designed failure to safety, redundancy and other SCEs | Driver logs<br>Access to site, underfoot conditions; site-specific hazards, site familiarity<br>Driver fit-for-work, drink/drug checks, rostering/fatigue/staff levels<br>Lone worker issues<br>Safety critical equipment and tasks |
| | Contractor & supplier selection and management | | Third-party contractor management, especially for supervision and competency of contract drivers | |
| | Incident reporting & investigation | | Multidisciplinary approach to investigation<br>Reporting and implementation | |

| | | Process Safety specialist | Overlap | Generalist OHS professional |
|---|---|---|---|---|
| | | | of investigation outcomes | |
| | Project delivery | | Schedule and accountability | |
| | Management of major emergencies and emergency preparedness | Site dispersion analysis, potential for escalation | Communication systems for tracking emergencies en-route;<br>Emergency management plans for truck/driver and site<br>Emergency management response | Post-incident management of road collisions |
| **Assurance** | Legislation & regulations | Process safety and design legislation, standards and codes | Safety, design, standards and codes | OHS legislation, standards and codes |
| | Audit, assurance, management review & intervention | | Audit of systems, processes and procedures related to tanker design and operation | |
| **Human factors** | Human factors | Design and specification of SCEs | Vehicle design, development of SCEs and procedures to ensure an integrated approach to design and operation | Design and specification of vehicle and work procedures |
| **Culture** | Safety leadership commitment, responsibility & workplace culture | | Act as role model in promoting process safety and OHS outcomes for operations and maintenance of tanker fleet through a multidisciplinary approach | |

# Appendix 3 Comparison of process safety and OHS management systems

This Appendix provides a high-level comparison of the management system elements defined in ISO/*AS/NZS 45001:2018* (SA/SNZ, 2018) *Occupational health and safety management systems — Requirements with guidance for use* with the process safety management system elements described in the American Institute of Chemical Engineers' (AIChE) Center for Chemical Process Safety publication, *Guidelines for Risk Based Process Safety* (CCPS, 2007). Note that specific references in ISO 45001 to "process" relate only to the administrative or management processes within a safety management system. Other process safety management system frameworks can be accessed from the Energy Institute (EI, 2022) and the Canadian Standards Association (CSA Group, 2022). All of these process safety frameworks are similar. The CCPS one has been used below for simplicity.

The alignment of system elements should not be read as implying a close comparison, but rather as indicative of areas where there is general alignment and an opportunity to integrate the management of both process safety and OHS.

Clause 6.1.2.1.f)1) of ISO 45001 is specifically included as it is the most significant reference relating to process safety design aspects.

The Elements in red are specific for Process Safety.

| **ISO 45001** (SA/SNZ, 2018) | | **Guidelines for Risk Based Process Safety** (CCPS, 2007) | |
|---|---|---|---|
| Based on the 10-chapter/element structure of Annex SL, ISO 45001 implements the *Plan, Do, Check, Act (PDCA)* cycle.<br><br>The first 4 chapters/elements form the background for the rest of the OHS management system, but are included in the numbering system:<br>1 Scope<br>2 Normative references<br>3 Terms and definitions<br>4 Context of the organization | | 20 Elements are each given a separate Chapter in the document) are grouped into four Pillars:<br>• Commit to process safety (1, 2, 3, 4, 5)<br>• Understand hazards and risks (6, 7)<br>• Manage risk (8, 9, 10, 11, 12, 13, 14, 15, 16)<br>• Learn from experience (17, 18, 19, 20)<br><br>The first 2 chapters (1 & 2) and last 2 chapters (23 & 24) of the CCPS Guidelines are not considered as specific Elements and are normally excluded from the Element numbering. | |
| **No.** | **Chapter / Element** | **No.** | **Chapter (Element)** |
| **5** | **Leadership and worker participation** | | |
| | 5.1 Leadership and commitment | 3(1)<br>4(2)<br>5(3)<br>6(4)<br>7(5) | Process Safety Culture<br>Compliance with Standards<br>Process Safety Competency<br>Workforce Involvement<br>Stakeholder Outreach |
| | 5.2 OHS Policy | | |
| | 5.3 Organizational roles, responsibilities and accountabilities | | |
| | 5.4 Consultation and participation of workers | | |
| **6** | **Planning** | | |
| | 6.1 Actions to address risks and opportunities | 3(1) | Process Safety Culture |

| | | | | |
|---|---|---|---|---|
| | 6.1.2.1 f)1) | the design of work areas, processes, installations, machinery/equipment, operating procedures and work organization, including their adaptation to the needs and capabilities of the workers involved; | 8(6)<br>9(7) | Knowledge Management<br>Hazard Identification and Risk Analysis |
| | 6.2 | OH&S objectives and planning to achieve them | | |
| **7** | | **Support** | | |
| | 7.1 | Resources | 5(3)<br>8(6)<br>12(10)<br>14(12)<br>15(13) | Process Safety Competency<br>Process Knowledge Management<br>Asset Integrity and Reliability<br>Training and Performance Assurance<br>Management of Change |
| | 7.2 | Competence | | |
| | 7.3 | Awareness | | |
| | 7.4 | Communication | | |
| | 7.5 | Documented information | | |
| **8** | | **Operation** | | |
| | 8.1 | Operational planning and control | 10(8)<br>11(9)<br>13(12)<br>16(14)<br>17(15) | Operating Procedures<br>Safe Work Practices<br>Contractor Management<br>Operational Readiness<br>Conduct of Operations |
| | 8.2 | Emergency preparedness and response | 18(16) | Emergency management |
| **9** | **Performance evaluation** | | | |
| | 9.1 | Monitoring, measurement, analysis and performance evaluation | 20(18)<br>12(10) | Measurement and metrics<br>Asset integrity and reliability |
| | 9.2 | Internal audit | 21(19) | Auditing |
| | 9.3 | Management review | 22(20) | Management review and continuous improvement |
| **10** | **Improvement** | | | |
| | 10.1 | General | | |
| | 10.2 | Incident, non-conformity and corrective action | 19(17) | Incident investigation |
| | 10.3 | Continual improvement | 22(20) | Management review and continuous improvement |