Process Safety

Protect@Contact

1

Introduction

To help make home the best place in world for all New Zealanders, we own, operate, and maintain plant and processes to generate energy. These have hazards which need to be managed safely.

On a daily basis we:

- handle potentially explosive substances such as natural gas, pentane, and hydrogen
- utilise the strong natural forces of wind, solar, geothermal and hydro power
- manage the complex process of converting these raw energy sources into electricity, involving geothermal wells, gas storage, high pressure steam systems, chemical batteries and large machinery rotating at high speed
- deliver electricity, natural gas and metering services to our customers.

Proactive management of these hazards and the risks they present is a key part of being able to generate and deliver energy in a safe and environmentally responsible manner to our customers. Delivering energy to New Zealanders safely is our priority at Contact and is critical to the ongoing sustainable operation of our business.

This guide explains our integrated approach to Process Safety as a way of managing our Major Incident Hazards. By 'integrated' we mean that Process Safety will:

- be applied together with other safety practices as part of overall Operational Safety
- be fully embedded in day-to-day processes
- form a core part of our generative safety culture
- be adopted for the long term.

What is Process Safety?

It's about keeping the process and the hazards, inside the equipment.

It's the collective name for the related measures, systems, procedures and policies which prevent incidents and/or protect people and the environment from the effects of major incidents.

" Any hazard which could cause an uncontrolled release of energy, toxic or hazardous material with the potential to cause a fatality or multiple fatalities, as defined by Contact's risk matrix, is called a Major Incident Hazard.

2

Process Safety: a key part of our safe operations

Reducing our process safety, occupational safety and environmental risks relies heavily on our Health, Safety and Environmental Management systems. By striving to follow due process, continuously improve, understand risks and build effective barriers, we do our utmost best to ensure our people stay healthy and safe.

This management system has provided a framework for improving occupational safety and through experience from actual incidents (also known as 'lagging indicators') we are driving continual improvement. However, while our industry has driven occupational and environmental safety incident rates down significantly, there is an opposing trend of catastrophic asset failures globally.

The way we are responding to the negative asset failure trend is through the adoption of Process Safety, which has a strong emphasis on using 'leading indicators'. Leading indicators are measures that tell us our systems aren't working as well as we'd like, before a failure leads to an incident.

The objective of Process Safety is to identify and proactively manage the hazards that have the potential to cause major incidents that harm or kill our people, contractors or members of the public, to harm the environment or damage assets.

Process Safety incidents are characterised by their low frequency but high impact, they can be highly publicised and can have a significant long term detrimental impact on the reputation and commercial performance of the organisation involved.

Generative Safety Culture

- Process Safety
- Health & Safety
- Safety from the System (Safety Rules)
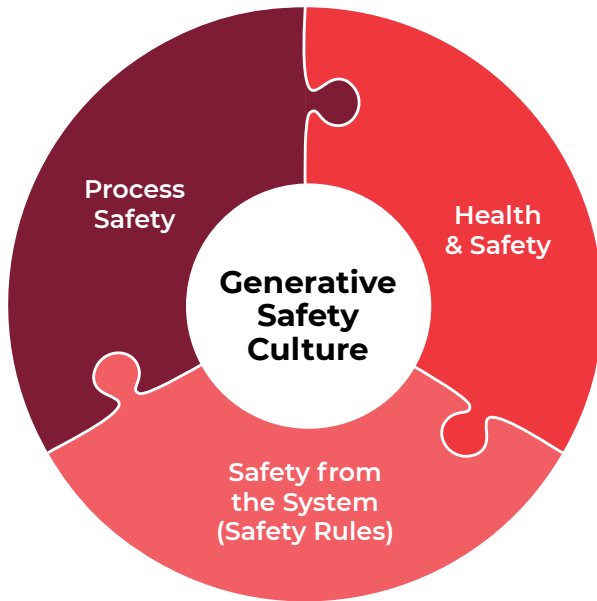
In response to significant incidents such as Texas City, Buncefield and Deepwater Horizon, Process Safety has become a key focus in the major hazard industries worldwide.

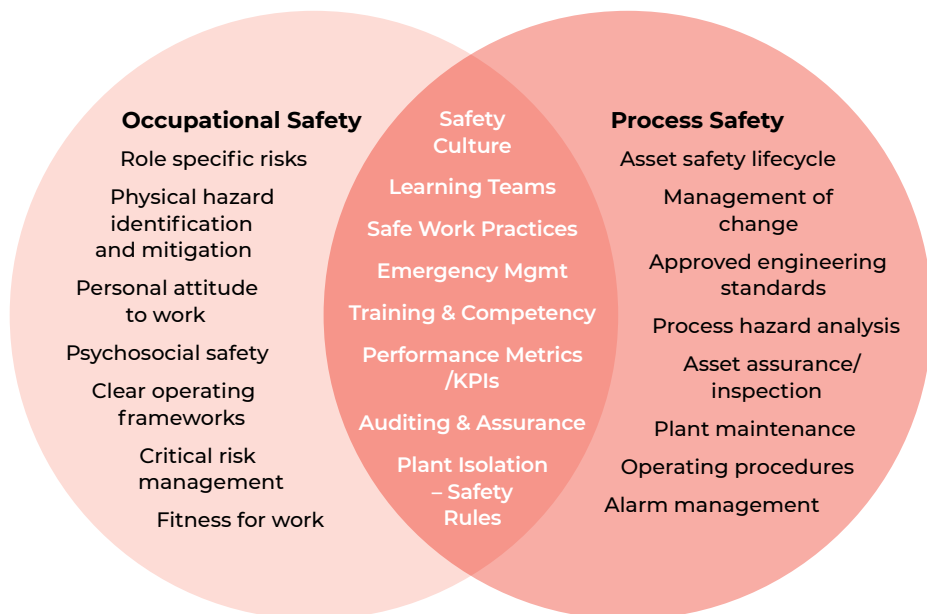In New Zealand, our regulator WorkSafe is also focused on the management of Major Incident Hazards.

Our aim is to integrate Process Safety with other established work practices to create a Generative safety culture and achieve our goal of safe work outcomes . All practices share common themes such as leadership, culture, communication, training and the need for Key Performance Indicators (KPIs).

> " Our industry is evolving with new technologies entering the generation mix as part of the energy transition. A disciplined approach to Process Safety ensures we identify and manage the major incident hazards associated with all of our generation assets.

What you need to know

- We are focused on improving our systems to ensure the safety of our people through effective Occupational Safety practices.
- As an industry we have seen a number of catastrophic plant failures globally. This is a 'lagging indicator' for deteriorating Process Safety performance.
- Process Safety incidents are low frequency but high impact, and a more proactive approach is required as it is not sufficient to wait for and learn from incidents.
- Process Safety does not replace other practices – it works together with our other safety management systems to support a Generative safety culture and achieve safe work outcomes.
- The objective of Process Safety is to prevent major incidents that harm or kill people, harm the environment or cause significant damage to our assets.

Occupational Safety

Role specific risks

Physical hazard identification and mitigation

Personal attitude to work

Psychosocial safety

Clear operating frameworks

Critical risk management

Fitness for work

Safety Culture

Learning Teams

Safe Work Practices

Emergency Mgmt

Training & Competency

Performance Metrics /KPIs

Auditing & Assurance

Plant Isolation – Safety Rules

Process Safety

Asset safety lifecycle

Management of change

Approved engineering standards

Process hazard analysis

Asset assurance/ inspection

Plant maintenance

Operating procedures

Alarm management

3

Your role is critical to Process Safety

You have a key part to play in ensuring Process Safety

Maintenance
"I carry out all routine maintenance as planned."

Engineering
"When designing and modifying plants, I will have asset integrity front of mind."

Leadership
"I will lead Process Safety and have it top of our agenda."

Operations
"I will focus on operating our assets within design limits and follow operating procedures."

Asset Management
"I target investments to the assets with the highest risks."

Everyone
"Where I see processes and systems that don't reflect the work being done or there are opportunities for improvement, I will collaborate with the process owner to update them."

This includes:

- Never being complacent, maintaining a 'sense of unease' – be aware of the hazards and risks that are present on your site and take time to consider what actions you can take to improve Process Safety.

- Communicating effectively, particularly when you are involved in hazardous operations.

- Playing your role in developing a process safety culture – encourage other employees and contractors to think about their role creating safe work outcomes.

- Attaining the competencies that you need to do the job, with a focus on skills which are safety critical

- Understanding the processes, procedures and instructions that apply to the activity you are doing, and challenging any that are incorrect or difficult to follow.

- Reporting any item of equipment that is difficult to operate, maintain, inspect or test or not operating as it should.

- Ensuring that all incidents and near misses are reported.

- Not being afraid to question things which just don't seem right.

4

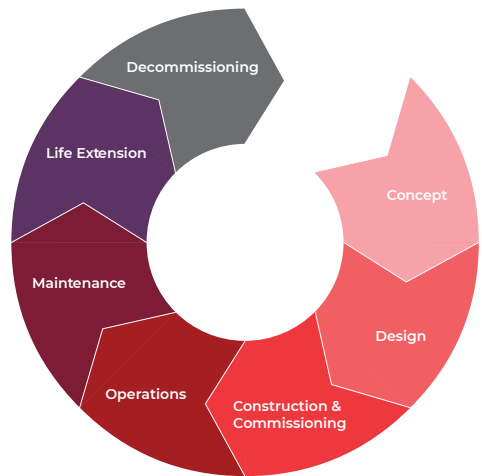# Process Safety is underpinned by good Asset Management

Successful Process Safety requires good Asset Management at all stages in the asset lifecycle from the initial concept and design phases through to construction, commissioning, operation, maintenance and all the way to decommissioning.

Along with many process based industries, Contact has adopted the internationally recognised approach set out in ISO 55000 as the foundation for Asset Management. These adopt a risk-based approach to managing assets through understanding asset related risks and putting in place appropriate mechanisms to manage them.

ISO 55000 has a strong focus on setting an overall asset management policy and strategy and then applying this throughout the entire asset lifecycle through:

- An organisational model that facilitates the implementation of the policy and strategy through clear direction and leadership;

- Employee awareness, competency, commitment and cross-functional coordination;

- Integrated information and knowledge of asset condition, performance and risks.

> "Poor design can make the safe, reliable and efficient operation of an asset more difficult. The early stages of the asset lifecycle are vital.

What you need to know

- Successful Process Safety requires good asset management at all stages in the asset lifecycle, from the initial concept through to decommissioning;

- Many process based industries have adopted international standards for asset management (ISO55000) that require an asset management policy and strategy to be set and applied at all levels within the business, and to all stages through the lifecycle of an asset.

5

Risk Management Process

ISO55000 promotes a risk-based approach to Asset Management which ensures all assets and hazards have been considered. An asset risk framework is used to identify and assess risks in order to put controls and investment in place to reduce these risks 'so far as is reasonably practicable'.

The framework is supported through regular workshops attended by diverse specialists from across teams such as operations, engineering, environment, maintenance, and health and safety.

Risk-based approach to Asset Management

1. Identify the plant asset and hazard being assessed
2. Evaluate consequences of failure event happening
3. Identify threats that could lead to failure event being realised
4. Identify and assess threat controls
5. Identify and assess consequence mitigations
6. Create actions to improve controls & mitigations
7. Review and report

1. Identify the plant asset and hazard being assessed
The first step in the process utilises the asset and hazard registers to ensure all assets and hazards have been considered. The combination of plant asset and hazard will lead to one failure event, which will be the focal point for the assessment.

2. Evaluate consequences of failure event happening
Based on the consequences defined in our risk matrix. The framework should be supported through regular workshops attended by specialists from engineering, operations, environmental, maintenance, and health and safety teams.

3. **Identify threats that could lead to failure event being realised**
What could cause the event or scenario to occur? There will be a number of different threats for each event.

4. **Identify and assess threat controls**
Each control is classified as either people, process, plant or recovery. The objective is that the controls reduce the risks from these threats so far as is reasonably practicable and in line with Contact's Risk Management framework. Controls can be considered as proactive or preventative measures which reduce the likelihood of the threat occurring.

5. **Identify and assess consequence mitigations**
Similar to preventative controls, mitigations are assessed in order to reduce the effect of the consequences, should the failure event occur. These mitigations will also be assessed to ensure the overall risk is reduced so far as is reasonably practicable. Mitigations are measures which would be used to reduce the consequence of the failure event. Part of assessing mitigations is to assess them as reasonable to be implemented. At Contact we use the So Far As Is Reasonably Practical (SFAIRP) test to ensure that we put out resources into mitigations that deliver the greatest risk reduction.

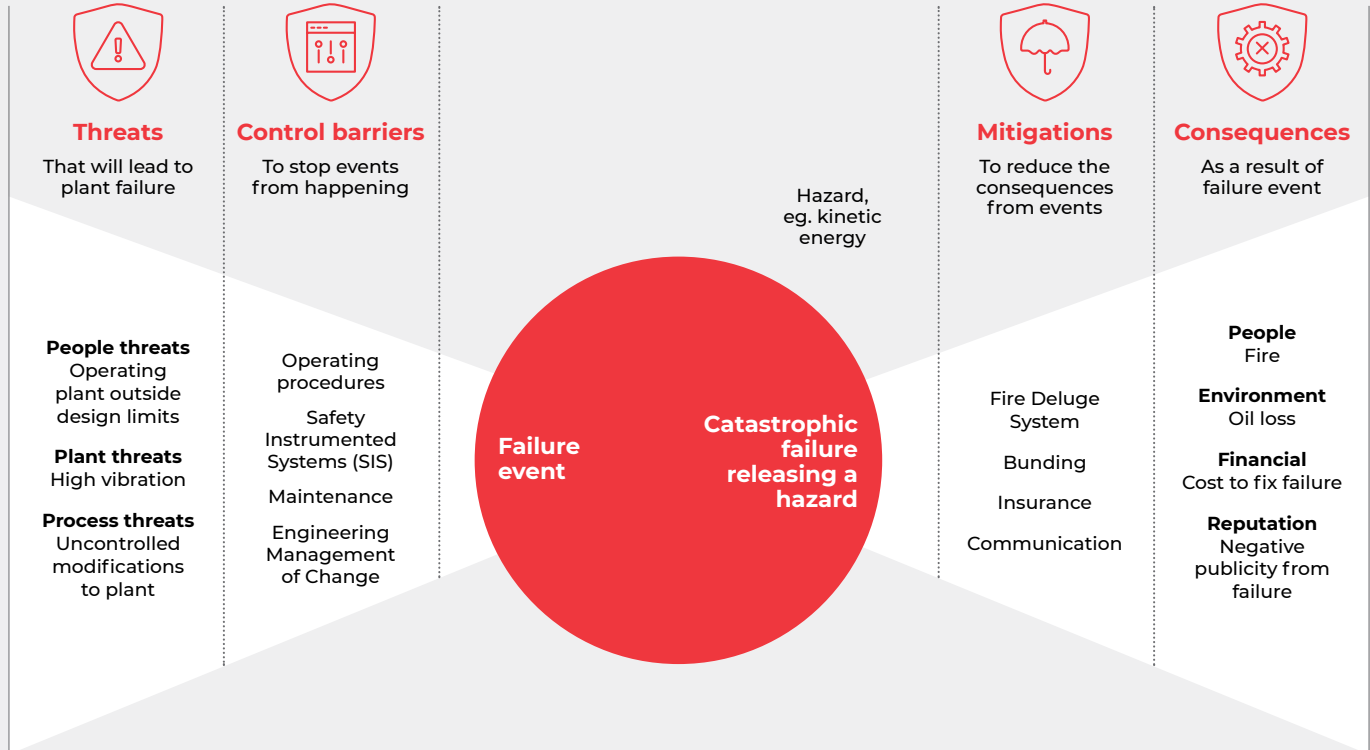6. **Create actions to improve controls and mitigations**
The assessment of controls and mitigations may lead to a number of actions being raised to introduce new controls or improve existing ones. These actions will be assigned to an action owner and tracked to completion through the system.

7. **Review and report**
Failure events are reviewed on a regular basis. We use Learning Teams, 5 Whys and other techniques such as Root Cause Analysis to review failures and update controls.

By categorising the likelihood and consequence of potential threats the risk can be assessed. As the Risk Framework is a common methodology used across all assets, the risk from different threats and plant assets can be compared and used to develop the overall plan for asset management and stay-in-business capital investment.

Bow tie diagrams are used to visualise the hazard being assessed

Threats
That will lead to plant failure

People threats
Operating plant outside design limits

Plant threats
High vibration

Process threats
Uncontrolled modifications to plant

Control barriers
To stop events from happening

Operating procedures

Safety Instrumented Systems (SIS)

Maintenance

Engineering Management of Change

Hazard, eg. kinetic energy

Failure event

Catastrophic failure releasing a hazard

Mitigations
To reduce the consequences from events

Fire Deluge System

Bunding

Insurance

Communication

Consequences
As a result of failure event

People
Fire

Environment
Oil loss

Financial
Cost to fix failure

Reputation
Negative publicity from failure

6

Our Process Safety Management System

Our approach to Process Safety considers the internationally recognised guidance HSG254, published by the UK Health and Safety Executive and the Centre for Chemical Process Safety (CCPS) – guides on Process Safety.

We are following five key systematic steps:

1. Hazard Awareness
The primary purpose of Process Safety is to manage Major Incident Hazards. The first activity is to identify all of the major hazards present in our business.

2. Process Safety Management Framework
For each hazard identified in Step 1 above, controls that prevent the hazard from harming people, the environment and our assets are mapped against this hazard. These controls are shown in our Process Safety Management Framework and fall into the categories of plant, process, people and recovery.

3. Leading Indicators
For each element of the Process Safety Management Framework, we establish metrics (known as Leading Indicators) that enable us to proactively monitor the effectiveness of its associated controls to provide assurance that they are performing as required. This is seen using a near real time Process Safety Key Performance Indicator (KPI) dashboard to give us visibility of the status of controls.

4. Lagging Indicators
Our incident management system is used to capture and classify incidents that are due to a failure of one or more risk control systems.

5. Governance
We put in place a governance process that ensures that both Leading and Lagging Process Safety Indicators, are reviewed regularly at all levels in the organisation, up to board level. Having visibility of the Key Performance Indicator dashboard and reporting performance facilitates these reviews.

> We constantly think about what could go wrong so we can build controls and barriers to prevent the event occurring.

1. Hazard Awareness

The day to day management of Major Incident Hazards has for a long time been a core part of our business. The way that assets have been designed and constructed, the processes that are followed on a day to day basis to operate and maintain them, and the skills and knowledge of our people are all geared towards keeping these hazards under control.
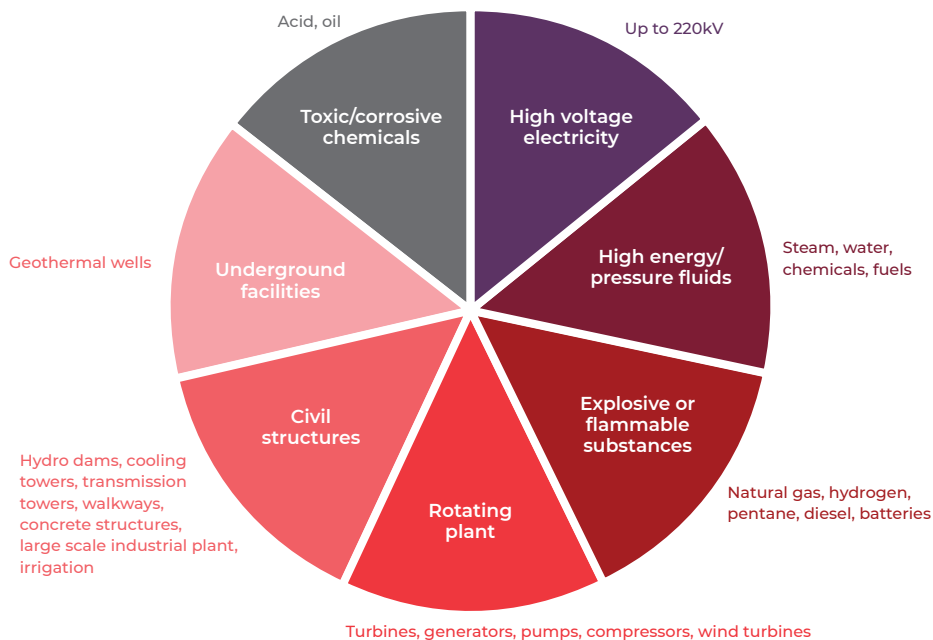
If these Major Incident Hazards are not managed effectively, they can put people, the environment and our assets at risk.

Process Safety requires that as an organisation we maintain a day to day awareness of Major Incident Hazards, along with strong awareness of the consequences of what could occur if we fail to manage them.

What you need to know

- A fundamental part of our business is successful management of a range of Major Incident Hazards on a day to day basis.
- Failure to identify these hazards and manage them effectively can have catastrophic consequences.
- Maintaining a 'chronic sense of unease' is not a bad thing – it keeps Process Safety front of mind.

Pie chart hazard categories (clockwise from top): High voltage electricity — Up to 220kV; High energy/pressure fluids — Steam, water, chemicals, fuels; Explosive or flammable substances — Natural gas, hydrogen, pentane, diesel, batteries; Rotating plant — Turbines, generators, pumps, compressors, wind turbines; Civil structures — Hydro dams, cooling towers, transmission towers, walkways, concrete structures, large scale industrial plant, irrigation; Underground facilities — Geothermal wells; Toxic/corrosive chemicals — Acid, oil.

2. Process Safety Management Framework

Our systems for controlling Process Safety risks need to be clearly identified. These are designed to manage the hazards present in our business to prevent them from harming people, the environment or our assets.

Our risk control systems have been identified within a Process Safety Management Framework which contains four interlinked high-level categories:

Plant – the primary objective when designing or subsequently modifying our plant, is the successful management of the hazards which are present.

In particular, the effects of the environment in which plant and equipment is operated and ageing processes (eg. corrosion or fatigue) must be considered.

Process – the processes that are followed to design, build, commission, operate, maintain and modify assets should be clear and practical. We will use common processes where possible to improve performance, supported by best practice guidance and systems.

People – ensure that our people have the right capabilities in terms of hazard awareness, competency, culture and supervision. To deliver this, Process Safety leadership should be part of our culture and language every day and good working practices should be recognised and shared.

Recovery – recovery processes which are put in place for plant, processes and people capabilities that mitigate the consequences should an incident occur. Examples of each include fire fighting systems, emergency plans and the awareness of emergency evacuation procedures.

> **Did you know:** The investigation into the 2005 BP Texas City refinery explosion, which killed 15 workers and injured more than 170 others, showed that failures in 12 separate risk control systems enabled the accident to occur. This included inherent issues in the design of the equipment (plant), failure to follow start up procedures (process) and the lack of supervision of a fatigued and overloaded operator (people).
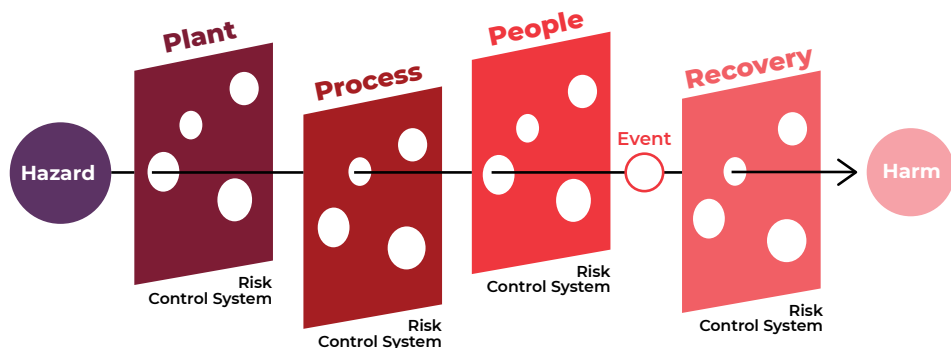
What you need to know

- We put in place systems of risk controls (or barriers) to manage hazards so that they do not result in harm to people, the environment or our business.
- Risk control systems fall into the category of either plant, process, people or recovery – by thinking in these terms we can make sure that we put the right mix of barriers in place.
- Due to the complex nature of the hazards, multiple barriers are required to manage them successfully.
- Investigations into major incidents typically show that multiple controls or barriers have been allowed to deteriorate, often over a long period, creating the conditions under which the incident has been allowed to occur.

Contact Process Safety Management Framework

Plant	Process			People	Recovery

Operations and Compliance Audit | External Audit | Integrated Internal Audit | Learning from events | Controlled Documents (Policies, Procedures, Standards)

Technical Risk Management	Safety Critical Systems	Alarm and Instrument Management	Maintenance Management	Operations Management	Staff Competence	Emergency Preparedness
Management of Change	Critical Systems	Process Control	Work Prioritisation, Planning, Scheduling	Startup/ Shutdown Procedures	Competency Assurance	Emergency Planning, Arrangement and Equipment
Plant Status Review/ Technical Risk Register	Emergency Supplies	Critical Instrumentation	Work Identification, Routine Plant Inspections	Routine Plant Checks	Leadership	
Strategic Spares	Fire Systems	Protective Systems/Devices		Routine Testing	Training Needs Analysis	Crisis Management
Engineering Standards	HV Electrical Systems	Alarm Systems	Work Execution	Shift Log/ Handover	Communications	
Technical Knowledge Management	Main Protection Systems	Operational Technology Security	Personal Risk Assessment	Safety Rules and Personal Risk Assessment	Staff Knowledge Management	Environmental Containment Systems
Design Review	Environmental Systems			Operating Limits/ Envelopes	Contractor Competency	
Asset Investment				Operational Risk Assessment		
Civil Asset Inspections				Third Party Activities		
Pressure Safety System						

The Process Safety methodology is commonly illustrated using the 'Swiss Cheese Model' where:

- The risk controls are depicted as a series of barriers that work to prevent a pathway from hazards to harm.

- Failures or deficiencies in the risk controls are then illustrated as holes in the barriers. These deficiencies may persist over a long period of time through a lack of focus on sustaining a particular barrier, or they can occur intermittently under specific conditions (for example during a start up process).

- When holes coincide in the barriers, the conditions are ripe for a major incident and this is illustrated as a pathway shown as a 'Major Incident Trajectory' that enables the hazard to cause harm.

3. Leading Indicators

Typically over 100 Leading Indicators measuring the health of the risk control systems will be identified to provide assurance that they are performing at the desired level. The key benefit of using Leading Indicators (as opposed to Lagging Indicators) is that they enable proactive action to be taken when performance of a Risk Control System degrades, before it fails completely.

" **We regularly review leading indicators.**

This is key to preventing Major Incident Hazard related incidents. Each Leading Indicator should have a clear definition, that is common across all sites, and targets for the required level of performance. The Leading Indicators are measured on a site by site basis (and also for key functions such as Engineering

or Asset Management) to enable full transparency of the outcomes. Technology is adopted to enable the majority of Leading Indicators to be calculated automatically on a daily basis and made visible to all staff through the Process Safety Key Performance Indicator dashboard.

Did you know: When a series of explosions ripped through the Buncefield Oil Storage Terminal in the UK, it caused an earth tremor that measured 2.4 on the Richter Scale

A total of 43 people were hurt as the blast destroyed nearby office blocks and fire engulfed 20 large storage tanks. It took 180 fire fighters to deal with what was the largest 'single seat' fire the world has ever seen and 2,000 people were evacuated.

What you need to know

- Monitoring leading indicators on a daily basis helps us to manage Major Incident Hazards.
- All leading indicators are specified in detail, including reasons for the indicator, target levels, and the way it is is calculated.

4. Lagging Indicators

Lagging Indicators are metrics that capture an occurrence where a barrier or control has failed in some way. These are illustrated on the Swiss Cheese Model as holes in the cheese. These indicators are important but not as effective as leading indicators for Process Safety management as they lead to reactive, post event actions.

A low threshold should be set for capturing incidents and near misses in line with industry guidance, adopting a tiered framework for classifying incidents. Incidents are also mapped onto the risk control systems that have failed to support integrated reporting of Leading and Lagging Indicators.

Major Process Safety Incident (Tier 1):

An actual uncontrolled loss of primary containment of a hazardous substance above the Tier 1 threshold, or a major loss of containment of electrical energy, or mechanical energy.

Significant Process Safety Incident (Tier 2):

An actual loss of primary containment of a hazardous substance above the Tier 2 threshold but below the Tier 1 threshold, a significant loss of containment of electrical energy or mechanical energy, or loss of all barriers where loss of containment has only been avoided by the absence of a challenge to the barrier system.

Minor Process Safety Incident (Tier 3):

A loss of primary containment of a hazardous substance below the Tier 2 threshold, minor loss of containment of electrical energy or mechanical energy, or degradation of the barriers in place to prevent a Major Incident Hazard.

To support this approach an incident reporting and investigation process is used and supported by our risk system to ensure that:

- Incidents including near misses are captured and the right people in the business investigate and identify how the incidents happened
- The investigation of all incidents is carried out to a minimum agreed standard in line with the severity of the incident set out in our Incident Management procedure

- Any actions that are identified during the investigation are logged and tracked through to completion
- The outcomes and lessons learned are shared with the person who reported the incident and also across our organisation.

What you need to know

- It is important to set a low threshold for capturing incidents in line with industry guidance to ensure that even minor Process Safety incidents are reported and investigated
- Understanding how incidents or near misses have happened will help us learn and improve on the way we manage Major Incident Hazards.

5. Governance

Our Governance arrangements drive regular reviews of Process Safety performance information at all levels in the business to identify trends and initiate the proactive actions required to prevent Major Incident Hazard related incidents.

Leading and Lagging indicators are a significant source of performance information, supplemented by other information such as asset risk management assessments, management reviews, audits (Engineering Standards ISO 55000, IS0-14001), accident and incident investigations, observations and benchmarking.

Governance takes two forms:

Formal Governance
Regular review meetings that are scheduled at all levels in the organisation from site level up to the Board. This puts in place formal ownership and accountability for Process Safety Management. The information that drives this process is fully transparent to enable all people to play their part in improving performance.

Culture

Alongside the formal governance process, all of our people and contractors are required to understand the hazards and risks evident in every day operations and report and challenge any concerns they may have about Process Safety. This culture is often described as maintaining a 'chronic sense of unease', and means always thinking about what could go wrong and never being complacent.

> ❝ **Our leading and lagging indicators will be available for all to see. This enables us to use them at all levels in our organisation for both formal and informal reviews of Process Safety performance.**

What you need to know

- A wide range of information should be reviewed on a regular basis at formal Governance meetings to ensure that Process Safety performance is understood and appropriate actions are taken and tracked where improvements are required.

- A Process Safety Dashboard is a key focus for the Governance process as it provides near real time Leading and Lagging Indicators as well as links to other key information sources such as the asset risk management assessments.

Process Safety is about protecting people, the environment and our assets from Major Incident Hazards.

Everyone has a role to play in helping to minimise the potential risks that our operational plant could cause harm to our people, the environment and our assets. This guide describes how, here at Contact, we use Process Safety to manage these risks and explains what Process Safety is, how it works, and how we can demonstrate that it is effective.

If we have an integrated Safety Management System, where Process Safety, Occupational Safety and Safety from the System are effective, this will support our priority of achieving a Generative Safety Culture that delivers safe work outcomes.

For more information contact
The Engineering Authority