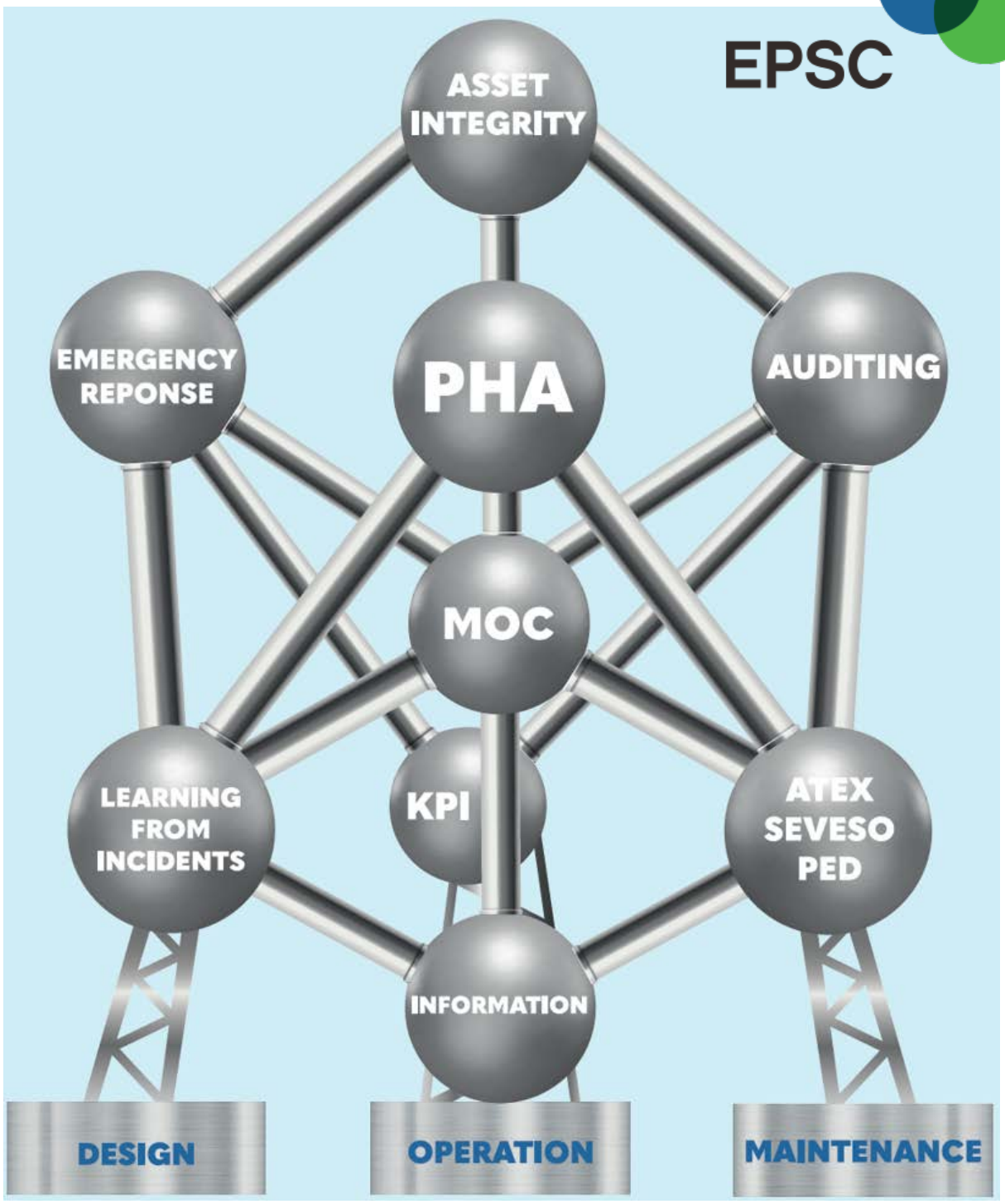
Process Safety Management
European Practice



Content

Author: Tijs Koerts, Operations Director EPSC
Reviewed by: EPSC (Board) Members

1. The reason for this booklet

The European way of doing process safety, as started in the sixties, has been well established and resulted in a clear legal framework with practical national implementation guidelines. Across the globe the European approach might be less well known and promoted and this booklet provides a useful description. One of the European characteristics is that the operator of the chemical sites as well as the regulator have a shared responsibility to protect society from chemical hazards. This requires a responsible operator and a competent regulator. A mature national auditing program is implemented in all the member countries of the European Community. It is one of the aspects where the European Seveso III regulation differs from e.g. the US OSHA standard.

This booklet aims to provide an easy readable summary of the process safety key aspects with a European view on best practices. It will help to give a good understanding of the basic principles for a wide range of people and it provides practical guidance for implementation. Furthermore, it can help organizations and sites with hazardous substances to set-up, benchmark and further improve their Process Safety Management (PSM) system.

The booklet starts with the explanation of some relevant concepts followed by two sections. The first section explains the key aspects of the Process Safety Management system in-line with the European Seveso legislation. The second section explains remaining important related safety topics and relevant legislation with their implementation practices.

2. Introduction to Process Safety Management (PSM)

Process Safety is about the potential for major accidents from hazardous substances, like chemicals or pressurized gasses. Typically one considers explosions, fires and toxic effects,

that might take place at a release. Process Safety aims to prevent or minimize injuries and fatalities as well as damage to the environment and production assets. Sometimes “Loss Prevention” is used, to manage chemicals to stay in their intended containment. Process Safety is relevant for companies that store or process, hazardous substances on operational sites. Transport of substances via pipelines, road, train, vessels, and planes, have their own regulations based on chemical hazard classification and will not be discussed here.

Three fields are relevant to control hazards of chemical processes of operational sites: the Design of the plant, the Integrity of equipment, and the Operation of the facility. These fundamental disciplines are essential for Process Safety, and they require their own organization with skilled specialists, guidelines and procedures.

Figure 1 Process Safety is founded on the disciplines: Design, Integrity and Operation

Process Safety Management (PSM) is a comprehensive framework consisting of subject elements, procedures, organizational structure, and competency to safely manage an operation that involves hazardous chemicals. Known examples of management systems are the DuPont’s wheel with 14 spokes and the CCPS 20 elements.

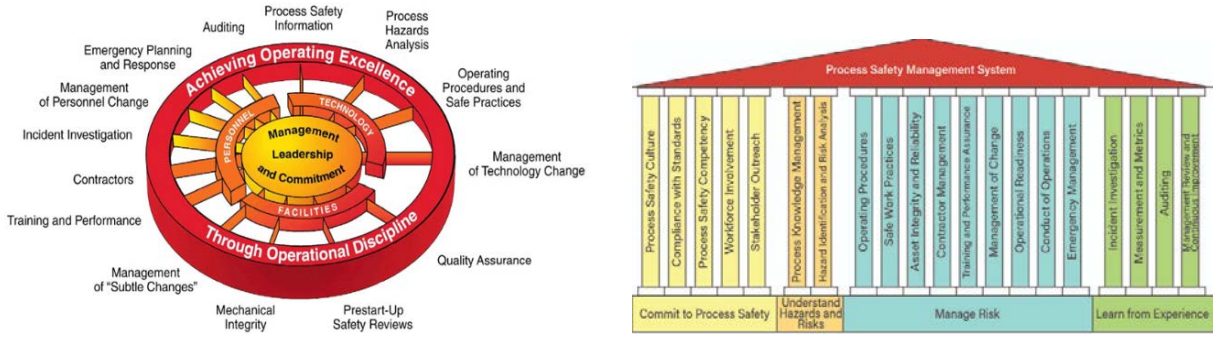


Figure 2 Examples of PSM systems: DuPont wheel and CCPS 20 elements

Here we introduce the European style of doing process safety, that has been less promoted. It has a strong focus on the key technical safety aspects as well as their best practices for implementation.

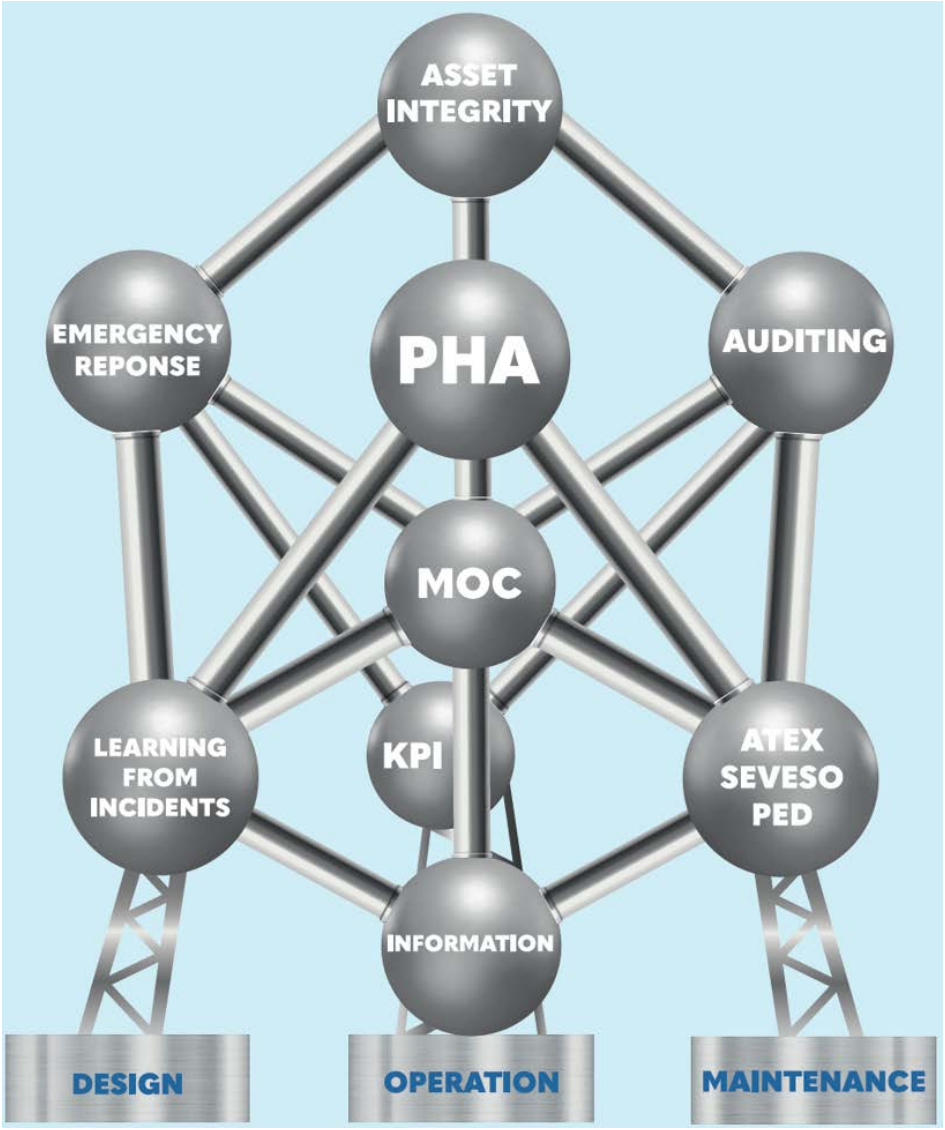


Figure 3 Visualization of the European Practice for Process Safety Management

The visualization of the European practice of Process Safety Management uses the Brussels Atomium structure. It shows the key elements of the management system, is based on the fundamental disciplines, and refers to some European regulations. It is also in-line with the European Seveso legislation that requires a management system with the mentioned elements.

3. European Incidents that shaped Process Safety

The following major process safety incidents had a large impact, and helped to establish process safety guidelines and regulations in Europe.

- Oppau, Germany (1920) Ammonium Nitrate explosion
- Fyezin, France (1966) Explosion of LPG storage spheres (Boiling Liquid Expanding Vapor Explosion or “BLEVE”)
- Flixborough, UK (1974) Explosion and fire after leaking cyclohexane
- Geleen, Netherlands (1975) Explosion and fire at a Naphtha cracker
- Seveso, Italy (1976) Runaway reaction with release of Dioxin from a reactor
- Chernobyl, Ukraine (1985) Explosion at a nuclear power plant releasing radioactivity
- Schweizerhalle, Switzerland (1986) Pollution of the river Rhine with pesticides
- Piper Alpha, North Sea (1988) Gas production platform sunk after explosion and fire
- Toulouse, France (2000) Ammonium Nitrate explosion
- Buncefield, UK (2005) Explosion and fire at an oil storage terminal
- Ludwigshafen, Germany (2016) Explosion after cutting in a live pipeline
- Tarragona, Spain (2020) Reactor explosion after a runaway reaction
- Leverkusen, Germany (2021) Explosion of a storage tank at a waste facility

This incomplete list of incidents, have impacted PSM legislation, guidelines and practices.
The European legislation on process safety is named after Seveso, a village in Italy, where a runaway reaction happened resulting in the release of dioxins to the atmosphere in a nearby chemical factory in 1976.

4. Difference between occupational safety and process safety

For a long time “Managing Safety” was primarily focused on managing occupational safety and health, with the target of avoiding injuries to workers. To support this, statistics have been developed such as lost time injury (LTI), and medical treatment case (MTC). These incidents are expressed in an occupational safety incident rate per 200.000 working hours. Managing safety was focused on reducing the incident rate, as well as the severity of incidents. This was realized by spreading good work practices, wearing personal protection equipment and by managing the behaviour of workers.
Managing the hazards of processes, chemicals and plant assets to avoid releases, followed by explosions, fires or toxic clouds, requires a different approach.
Therefore, PSM has been established as a separate field of expertise managed with a framework, different from occupational safety and industrial hygiene.

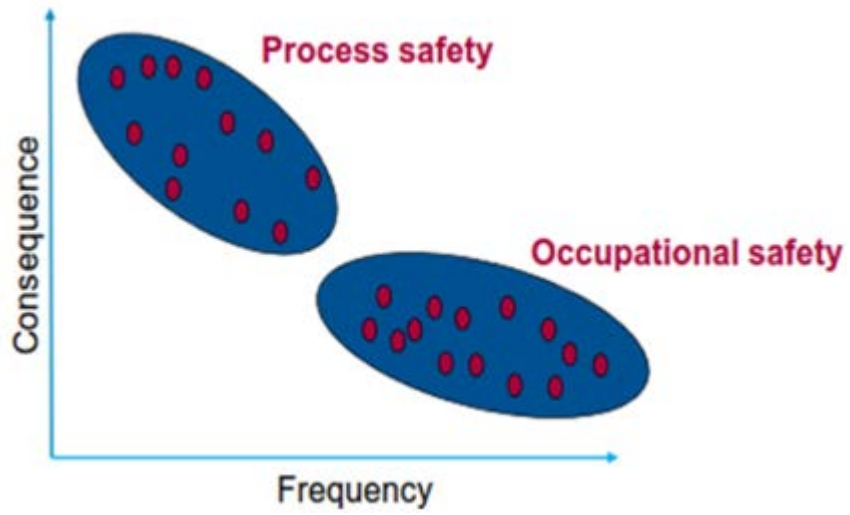


Figure 4 Difference between process safety and occupational safety

While occupational incidents are typically less severe (recoverable) and have a relative high likelihood of occurring, process safety incidents can affect a much larger area and number of people, eventually involving multiple fatalities and impact on the communities. Typically, the probability of these events is much lower. The low frequency of process safety incidents might lead to a perception of low danger resulting in an underestimation of the hazards. Also, Process Safety requires a deep understanding of the chemicals and technical processes. This is why process safety requires a different approach and why PSM should have its own experts, management system, requirements, and organization at sites with hazardous chemicals.

5. Measuring Process Safety

The incident at the Texas City Refinery in 2005 revealed that process safety was not defined well enough, and that its performance was not measured with appropriate metrics. Therefore, a metric for process safety was developed with the main lagging indicator: Loss of Primary Containment (LOPC), related to uncontrolled releases from the process. The spill size and the chemical involved determine the incident classification according to either the API-754 or ICCA/CEFIC standard. Also the importance for good leading indicators is described in these standards. Since 2018 EPSC has benchmarked the industry performance on process safety, using the LOPC rates of companies that classify leakages according one of these standards.

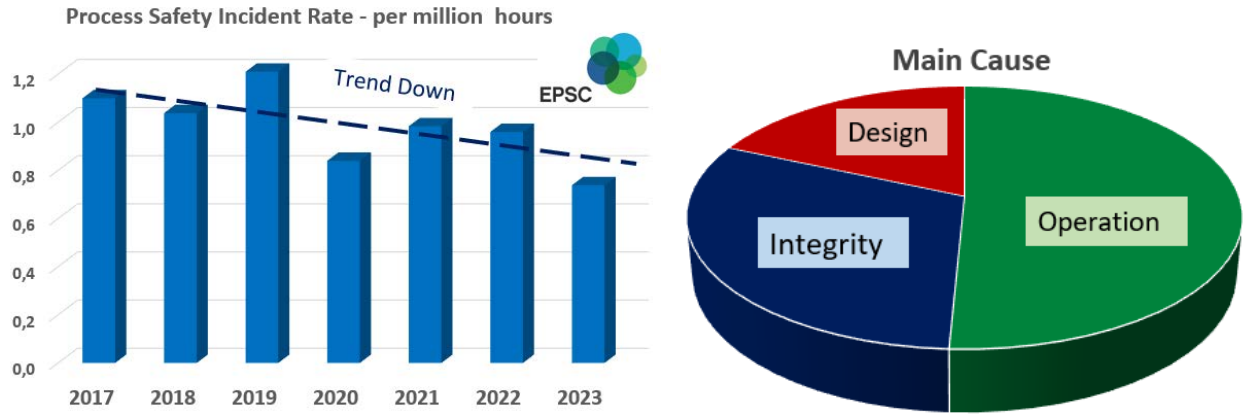


Figure 5 Industry performance on process safety incidents per 1 million working hours and the main cause in categories Operation, Asset Integrity and Design

6. Hazard and Risk description

The terms Hazard and Risk are central in process safety management and they need to be understood well. As long as hazardous substances are on site, risk is typically not zero. The risks need to be estimated and managed to an acceptable level. Current PSM systems are primarily 'risk based'. Hazard and Risk are explained as follows:

Hazard is related to a source of energy in sufficient quantity to do harm. This can be from a chemical (Petroleum, Ammonium Nitrate, Phosgene) or physical state (high pressure steam, high velocity turbine wheel). Nuclear or biological hazard sources are usually not included in PSM. Uncontrolled release can result in fire, explosion, or toxic cloud, that can impact people, environment, or assets. The consequence severity is typically classified in categories.

Figure 6 Examples of Hazards (uncontrolled releases): Heat radiation from a fire, Explosion pressure wave, Chemical Exposure, Environmental Pollution, Kinetic energy release.

Risk includes, besides the consequence, the likelihood of the hazard to occur. Risk of an event includes the Probability (assumed frequency) of the damaging event. One often uses simply **Risk = Consequence x Likelihood**. A risk matrix can be used to classify scenarios based on their potential for hazard and the likelihood of occurrence.

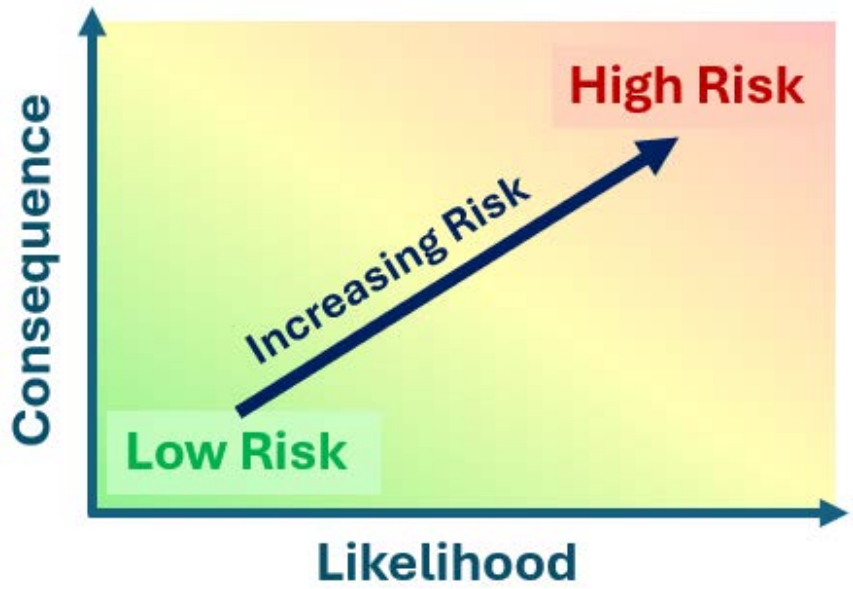


Figure 7 Risk has two components: Likelihood (how often) and Consequence (how bad)

7. Part 1: The Process Safety Management System

As mentioned, different process safety management systems have been established. They all have chapters or elements, and a number of these are essential elements that are always addressed. These key elements are: Process Safety Information (PSI), Process Hazard Analysis (PHA), Mechanical or Asset Integrity, Management of Change (MOC), Emergency Response, Learning from Incidents, and Auditing and Performance. The European SEVESO III legislation, requires a safety management system that contains these elements.

These essential elements for PSM are discussed in more detail in the following chapters. When starting a PSM system it can be helpful to first focus on these essential elements.

8. Process Hazard Analysis – PHA

Hazardous operations must identify, and evaluate all the hazards of their process that contains hazardous chemicals. The following questions need to be addressed:

- What can go wrong? (initiate an incident)
- How bad is it? (potential consequences)
- How likely is it? (frequency)
- What measures can reduce the risk to an acceptable level? (barriers)

8.1 Chemical Hazard Analysis

Before starting a PHA, the reactive nature of the chemicals involved need to be understood. Chemicals in reactors and storage vessels can react or decompose. When energy is released this can result in a run-away reaction followed by an explosion. Therefore, all reactive hazards must be identified and quantified. Energy release (from enthalpy change) can be calculated when the reaction is known, or practically measured in small quantity by Differential Scanning Calorimetry (DSC). Normal and abnormal process conditions (like increased temperature) should be considered.
Furthermore, it is good practice to identify with a so called "Chemical Matrix" the hazardous chemical combinations that can react to produce unwanted energy or toxic gases. Their accidental mixing has to be avoided.

8.2 HAZOP

Trevor Kletz stated: "a hazard not identified is a hazard not analysed" and to do so the HAZardous and OPerability study (HAZOP) was developed since the sixties of last century. This best practice is used to identify all hazards, in a very systematic way, considering all deviations in the process using guidewords such a "low flow". It is performed by a multidisciplinary team that includes specialists from process design, operation, maintenance, safety and is led by a HAZOP leader. The potential consequence and barriers (to avoid the incident) are documented for each deviation. When the remaining risk is considered high, a recommendation is made to further lower the risk. Other PHA techniques exist and can be applied, as long as they identify and evaluate the hazards.
Some aspects of the PHA element execution include:

- Operation units can be classified based on the amount and hazard of chemicals involved (e.g. high, medium or low risk).
- Units should have a periodic PHA review, the frequency can depend on the hazard classification of the unit and the number of process changes.
- The potential severity of the consequence for each scenario is identified by the HAZOP team.
- The high consequence scenarios, as identified in the PHA, can be used to further assess whether the barriers or protection layers are sufficient. Layers of Protection Analysis (LOPA) can be applied for such high consequence scenarios.
- Action items from PHAs should be tracked to completion, and a metric on the open actions is made available to management.
- The HAZOP team should be trained in the methodology and a highly-knowledgeable professional should lead and document the studies.

8.3 Risk Classification and Risk Criteria

To identify whether the risk is acceptably low, a risk matrix can be applied. Here, the probability and the consequence category of potential scenarios are listed in a table.
It is a corporation's legal responsibility to define a risk matrix with specific risk criteria for safety and environment. Some companies also include business loss, or asset damage, that

remains their own responsibility. The engineers and operation leaders can then apply the matrix to determine the risk for a specific scenario.

Risk Matrix Example				Probability in times per year						
Consequence	Class	Safety	Environment	1/100.000	1/10.000	1/1000	1/100	1/10	1	10
	E	Multiple fatalities, major explosion	Community evacuation, international boycot							
	D	Single fatality, Large fire	Large toxic release, Site evacuation							
	C	Serious Injury, Large leak	Permit violation, Fine							
	B	Small injury, Limited leak	Reportable spill							
	A	Near miss, First Aid	Near Miss, Low impact							

Figure 8 Example of a Risk matrix with criteria for safety and environment

Risk matrices are often visualised with coloured areas which have to be clearly explained. For example: Green for Acceptable, meaning the risk is sufficient low for the potential harm; Yellow for Tolerable, meaning the risk should be reduced to become acceptable: apply ALARP (As Low As Reasonably Practicable); Red for Unacceptable, meaning the risk is too high, the operation is not safe and needs short term improvement by adding barriers, redesign or stop the process.

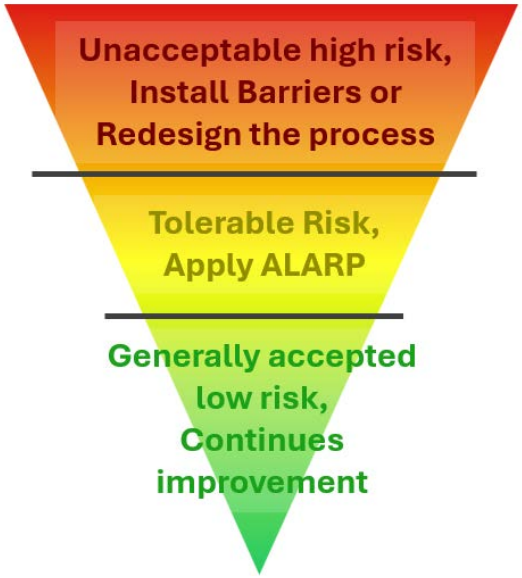


Figure 9 Explanation the colours of the risk matrix

8.4 As Low As Reasonably Practicable – ALARP

Risk matrices can have a yellow area indicating a tolerable risk of a scenario. For such tolerable risks it is appropriate to apply the As Low As Reasonably Practicable or ALARP principle. To do so, one considers the next logical measure to further lower the risk. The cost

and effectiveness of these measures can be taken into account in the evaluation, to determine whether or not to install the additional measure. ALARP can be well used to prioritise safety measures and budget planning for risk reducing improvement projects.

8.5 Scenario based Barrier Management

At a hazardous chemical facility, the risk can typically not be reduced to zero as long as hazardous chemicals are on site. Therefore, the risk reduction approach for hazardous scenarios is, to add sufficient protection layers to lower the likelihood, and with that the risk of the scenario, to an acceptable low risk level. This is called Risk Based Management. Scenarios can describe the pathway from something that goes wrong (a deviation, like a valve is placed in the wrong position) up to the worst, but credible, consequence. Barriers are identified and implemented that are intended to avoid the incident from happening. This scenario thinking is described in the so called “Swiss Cheese” model, in which the layers of cheese contain holes that represent the possibility of failure of the barriers.

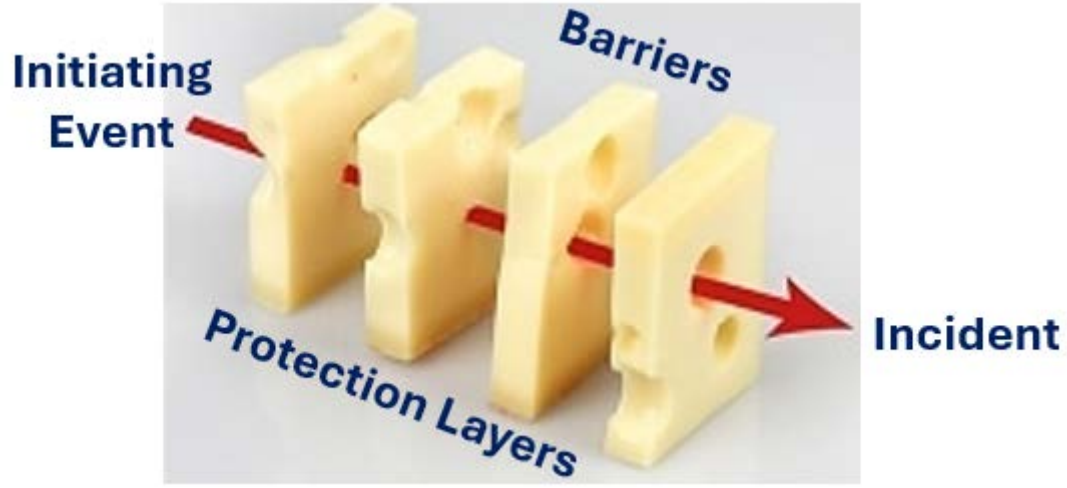


Figure 10 Swiss Cheese Model or Barrier Based Scenario Thinking. The holes in the cheese slice symbolize the possibility that a barrier can fail.

- The Initiating Event describes what goes wrong, like a valve is placed in the wrong position. The initiating event has a likelihood to occur.
- The Incident describes the release and the consequence, like an explosion. The Consequence has a severity that can be classified using a risk matrix.
- The Barriers can be safety systems or procedures with the intention to prevent or mitigate the incident.
- The “Bare Risk” is determined by the combination of consequence severity and likelihood of the event.
- The “Mitigated Risk” includes the reduced likelihood of the accident due to the Barriers.
- The holes in the cheese symbolize the failure possibility of the barrier.

The Seveso Legislation requires that chemical sites have documented and analysed the relevant scenarios in this way.

8.6 Layers of Protection Analysis (LOPA)

Layers of Protection Analysis uses the barrier thinking and applies a semiquantitative analysis. The initiating event (something goes wrong) has a likelihood for occurring (initiating frequency). The consequence has a severity that can be classified (e.g. a single fatality). In LOPA the barriers are called Independent Protection Layers (IPLs), that can fail. IPLs need to be independent from other barriers and the initiating event, they need to stop the scenario or avoid the consequence, and they need to be validated (tested in the field).

The likelihood of a scenario event and the failure rate of the barriers are typically not exactly known. One works with a conservative estimation of these in a so called semiquantitative risk analysis or LOPA.

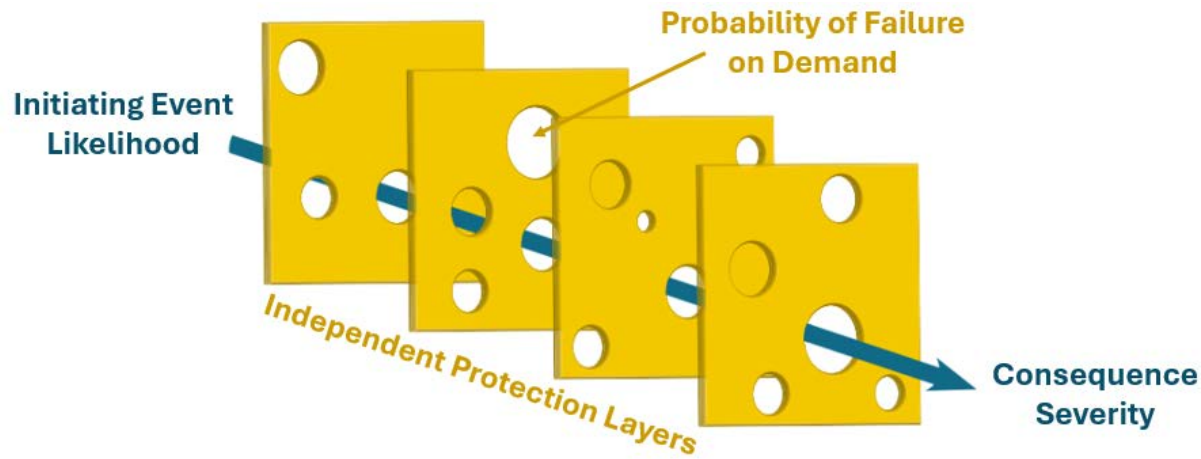


Figure 11 Layers of Protection Analysis (LOPA)

The likelihood of the initiating event is taken as a conservative order of 10. (e.g. a sensor fails maximum once per 10 years). The barriers or Independent Protection Layers (IPLs) have a reliability. The failure likelihood is described in the Probability of Failure on Demand (PFD), which is also estimated in orders of magnitude: e.g. a safety system fails a maximum once per 10 times. The failure rate corresponds to the Safety Integrity Level (SIL) of the barrier or safety system.

8.7 Bow-Tie

To visualise scenarios with barriers, Bow-Tie has become popular. While operation people typically do not read a HAZOP report, the visualisation of the key scenarios in a plot can be very helpful, to them as well as authorities.

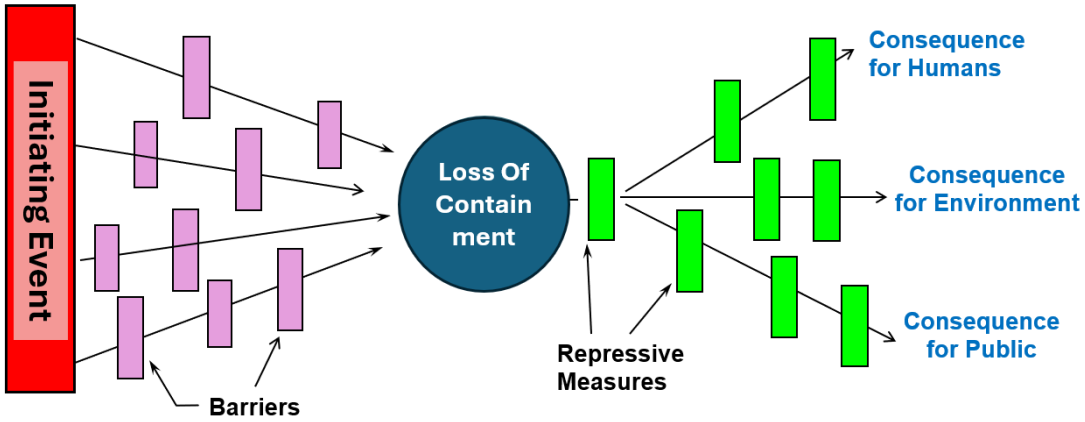


Figure 12 Bow-Tie figure showing scenario's in a plot

The centre of the Bow-Tie shows the Loss Of Containment (LOC). The left side shows the threat (or initiating event) that can result in the leakage as well as the barriers that prevent the leakage. On the right side of the Bowtie, repressive measures are mentioned to mitigate the effect of the release .

8.9 Safety Integrity Level – SIL

As barriers or safety systems can fail, it is important to design them well and understand their reliability, that is expressed in a SIL rating. The Safety Integrity Level relates to the Probability of Failure on Demand. One uses full orders of 10 to describe the reduction factor: a SIL 1 protection layer fails maximum in 1 out of 10 demand situations, a SIL 2 safety system fails maximum once in 100 cases, and a SIL 3 once per 1000.

SIL classification is well developed for instrumentational safety and described in the ISO IEC 61511 standard. SIL classification of safety systems can be conducted during a LOPA study using the risk matrix, or one can use the table from the mentioned standard. The electrical engineer can then design and implement the safety system to realize the required integrity level.

Figure 13 Safety instrumentation system with typical components

A Safety Instrumentation System (SIS) or interlock has a sensor in the process, a logic solver (like a safety PLC), and a final element (e.g. a valve that closes). Automatic protection of the process based on such an instrumentation loop, requires regular testing, in-line with the SIL level.

9. Asset Integrity

It is important that installations work as they are designed. The functionality of critical plant equipment needs to be validated and maintained through, manufacturing certificates, regular inspections, testing, and repairs. Safety critical equipment has to be identified, for which a PHA or a criticality study can be used. It includes mechanical items (static & rotating) as well as electrical systems (including their software). All “safety critical equipment” from the hazardous operation gets a number in the maintenance data base and a tag plate in the field. Examples include: electrical safety devices, Pressure Safety Valves, Rupture Discs, Check-valves. A colour code or tag identification (e.g. starting with Z) can help to make the criticality equipment visible to all. Each safety critical equipment will have a defined maintenance protocol and a test frequency. When an item is due for inspection, the maintenance system typically generates a work-order for that. Maintenance personnel will take care of the execution and report back on findings.

Some aspects of this discipline:

- Safety critical equipment is identified and numbered. It has an inspection/testing protocol and a set frequency for that.
- Expertise exists within the organization on static, rotating and electrical equipment.
- Maintenance planning is well discussed and aligned with operations.
- Backlog on maintenance needs to be measured and reported to site leadership.
- Overdue inspection on safety critical equipment, should be risk assessed and approved.
- Inspection and testing of pressure equipment is conducted by certified specialists from Notified Bodies, accredited by state. Such inspectors can apply Non Destructive Techniques (NDT) to measure wall thickness, cracks and the quality of welds.
- Bypassing of safety systems is controlled by a procedure that includes authorization and temporary measures.
- Repairs are made with identical parts (replacement in kind). If not, potential new hazards need to be identified and evaluated with an Management of Change (MOC) process.
- Equipment ageing and relevant corrosion mechanisms are understood, and this is validated in the field.

Previously, Asset Integrity was called Mechanical Integrity with a strong focus of “keeping the chemicals in the equipment”. Electrical equipment as well as software can also be safety critical and need their own testing and inspection protocols.

9.1 Reliability Centred Maintenance (RCM)

To determine the required reliability of equipment, a criticality study can be applied. Here consequences are identified when the equipment fails. With set risk criteria (from a risk matrix) an accepted likelihood for occurrence is determined. From this the required reliability of the equipment is determined. With understanding of the failure mechanisms,

and information from the supplier, a solid inspection protocol and frequency can then be set.

9.2 Risk Based Inspection (RBI)

To determine proper inspection frequencies for pressure equipment, Risk Based Inspection (RBI) can be applied. It requires certified specialists and understanding of wall thickness deterioration in time, that is mechanisms of erosion, corrosion, and damages. With strict guidelines and approval from authorities (in-line with national legislation) one can e.g. deviate from a prescribed inspection regime interval for pressure vessels.

10. Management of Change (MOC)

When a change is made to an installation, new hazards can be introduced. The MOC process aims to identify new hazards related to the change, and define appropriate measures to make sure new hazards are well-mitigated. A change can be defined as anything except for a "replacement in kind". Changes can include e.g. large projects, new equipment suppliers, changes in personnel, which all require their own analysis. The MOC process as discussed here, focuses on physical and electrical changes to systems that contain hazardous chemicals.

- All plant changes are identified, assessed and approved.
- Plant changes need a well-defined and detailed scope, e.g. made by a process engineer with the input from operations, maintenance, suppliers etc. It includes a modified P&ID.
- On the basis of the scope, the potential effects of the change can be identified and evaluated in an appropriate hazard analysis. This can be best conducted by a team. It is good practice to involve e.g. process technology, project engineering, maintenance and production in the MOC review. The actions from the analysis, to assure the modification can be safely introduced, will be documented.
- Checklists can be used to validate that specific hazards/aspects are addressed, and to indicate the documentation that needs to be updated.
- Implementation can be done of the basis of a detailed scope eventually with the help of a contractor.
- Prior to bringing the modifications on-line, validation of completeness on all aspects of the MOC has to be accomplished. Only then, formal handover to operations can be done, that should be authorized by e.g. the plant manager. The best practice to validate the operational readiness is called pre-startup safety review.

10.1 Pre-Startup Safety Review (PSSR)

Start-up of a new plant, or after a modification or turn-around, has led to severe incidents when it is not well prepared. Checking that the plant is ready for start-up with modified conditions is a critical step that requires a validation process. First the completion of the work in the field, like mechanical and electrical completion, must be done with the

contractor. Further, production needs to be prepared by updating the procedures, and training all shifts. Once these steps are completed, the PSSR can be executed by a team that includes at least the project engineer, the process engineer, the contractor, and operations, maintenance and EHS representation. The PSSR typically uses a checklist and validates the critical things like “are all PHA action items, as defined in the MOC, completed”. PSSR includes a documentation check, and a field tour with the team, where at the location all remaining items that need completion are noted. When all the critical items are completed, the modified plant can be officially handed over to production. After that, production is responsible to start-up and operate the new situation safely.

11. Emergency Response (ER)

When a release has occurred, the operational team must be prepared to minimize the impact. This involves identification of key scenarios that require preparedness. The large scenarios with flammable substances are used to determine the requirements of the fire response equipment and organization. A similar process exist for toxic gas clouds. The emergency response requirements are typically agreed with authorities and documented in the permit to operate the plant. Necessary fire response equipment and organization can come from a nearby central fire brigade, or provided by the site. Critical equipment for emergency response needs to be identified and maintained. Some further aspects of this element are:

- Drills are defined, executed and learnings are followed-up.
- ER personnel are identified and trained.
- ER equipment is available and regularly tested.
- External fire-fighting services are agreed upon and joint ER testing is conducted.
- Escape plans are defined and all site personnel are trained.
- For toxic gas clouds, community emergency response is set-up.
- Block-In systems are defined to limit leakages from systems. Motor operated valves (MOV), that can be closed from distance, and can be part of automated ER procedures.
- For plants with pressurised flammable gases, an ER procedure may include blocking the gas intake at the battery limit and depressurizing the plants to a safe disposal system like a flare.

12. Learning from Incidents

In the event that something went wrong, it should be reported and investigated so that repetition in comparable situations can be avoided. This requires an organizational culture without fear to report, where people feel at ease when they bring-up situations that didn’t go well. Such an open learning culture can be a strong basis for continuous improvement. Element aspects include:

- A system exists where incidents and near misses can be easily reported. These are classified and will be accurately followed-up.

- Incidents with high potential are investigated accordingly by a team.
- Direct and root causes will be identified using Root Cause Analysis (RCA).
- An appropriate incident report is made that is shared with all relevant people in the company.
- Actions are identified to avoid recurrence.
- The incident findings and actions are presented to and discussed with management. The improvement actions are agreed and related resources identified and made available.
- A list exist that includes the status of the defined improvement action and the responsible person.
- Metrics exist on overdue incident reports and overdue action items from incident reports. Management drives actions to completion.

When well implemented, learning from incidents and near misses can be a strong driver to realize “Continuous Improvement”.

13. Process Safety Information

Availability of relevant technical information and documents is essential for Process Safety. The chemical properties and reactions, including their thermodynamics and kinetics data, have to be documented. The Piping and Instrumentation Diagram (P&ID) is an essential process description as it is the basis for hazard analysis, plant changes, and equipment isolation plans. P&ID’s should be “as built”, that is describe the actual plant status. Furthermore, it is good practice to have an technology file that describes the technical details of all equipment, that can for example include the scenarios used for relief vent sizing.

In addition, electrical equipment, alarm settings, and software programs need documentation that are kept updated in case of changes. Relevant documentation requires an owner, that is responsible for its quality.

As documentation might not be the most interesting part of an engineering job, it needs to be supported with discipline and culture.

14. Auditing and Key Performance Indicators

The management system is not meant to be a set of procedures in a filing cabinet and will only work well when its functioning is validated. For this purpose, internal audits, corporate audits, and external audits (by authorities or external specialists) can be used. Good audits are typically performed by experienced people that have an understanding of the work process. Leadership needs to be interested and informed on the audit results. They are responsible for developing a plan to close the audit gaps. Further aspects are:

- An audit schedule exists, including audits by the site, by corporate experts, by authorities, and other external bodies.
- Audit results are presented and discussed with management.

- Audit recommendations are documented with an owner and a completion date.
- Overdue audit actions are reported to management.
- Trained Auditors are available.

To manage process safety performance, a dashboard with leading and lagging indicators is helpful, summarizing important data from relevant departments. Leading indicators are relevant parameters, while leakage has not yet occurred. Examples of leading indicators are "the number of inspections on safety equipment that are overdue" or "the number of open recommendations from Process Hazard Analyses". The status on the Key Performance Indicators (KPI's) of the important process safety elements are made available to leadership, who can discuss them and assure follow-up.

Dashboard	Target	Q1	Q2	Q3	Q4
Parameter 1	A				
Parameter 2	B				
Parameter 3	C				
Parameter 4	D				

Figure 14 Dashboard with Key Performance Indicators to monitor and manage process safety performance

15. Part 2: Process Safety relevant topic and practices

The following chapters describe practices on other topics, that need to be addressed to manage Process Safety. Besides technical topics, aspects related to humans, organization, culture, relevant to support the avoidance of major incidents are included here.

15.1 Process Safety Culture

A strong process safety culture is considered essential to obtain a good process safety performance. Generally, strong conviction of leadership is essential for a strong culture. This, however, is not easy to create, as saying "Safety is a value" by itself, does not create the perception of importance. The behaviour of leaders and their interest and commitment to process safety, helps to create a positive culture. Further the value for safety must be embedded in all layers of the organization.

The safety culture of a company or at a site can be evaluated using the so-called safety ladder as shown (developed within Shell). It consists of different maturity stages. It can be helpful to validate whether an organization has reached the desired state and where there is room for improvement.

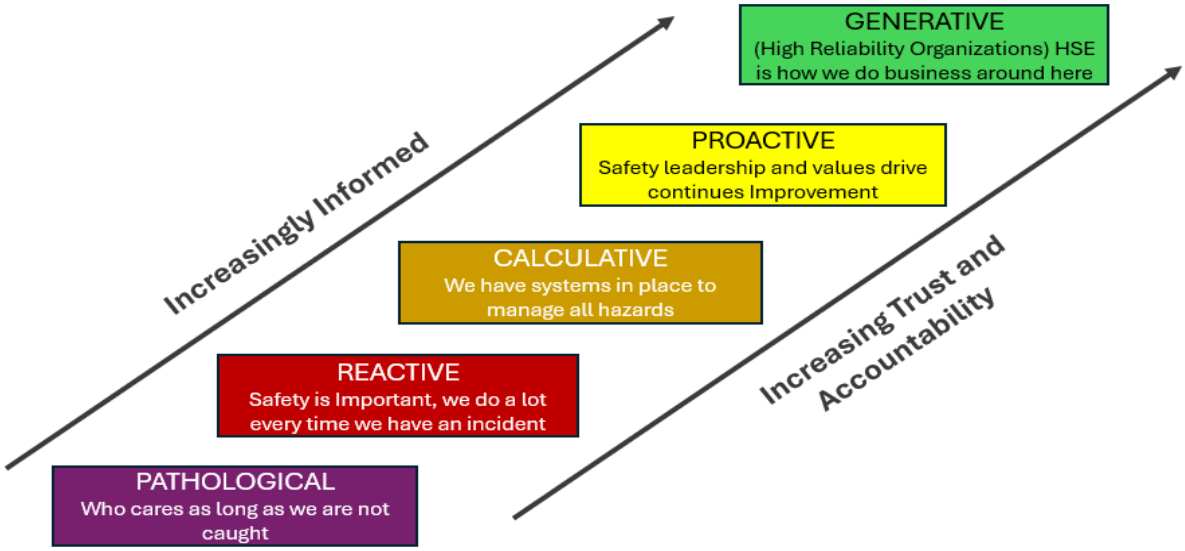


Figure 15 Process Safety Ladder according to the "Hearts and Minds" model

15.2 Process Safety Leadership

It is important that senior management and site leadership in a company have and show a strong commitment to safety, and establish safety as a value, that cannot be compromised. It is not easy to create that in-depth conviction within leaders, that is often developed by necessity, following a serious incident. Some aspects that can help to strengthen process safety leadership in managers are:

- Good understanding of the site main hazards and barriers.
- Discussion with people in the field to understand their problems.
- Involvement in incident and near miss investigations and support for improvement.
- Showing interest in aspects of the PSM system. Discuss the PSM KPI dashboard in-depth using "Embrace the Reds and challenge the Greens".
- Visible commitment that is regularly expressed in company meetings.

15.3 Process Safety Fundamentals

As shown earlier, most of the process safety incidents with chemicals have a cause that is related to how the facilities are operated. A management system is sometimes abstract and not particularly helpful for the day to day problems of operators and mechanics. Process Safety Fundamentals have been developed to create operational process safety excellence. EPSC has described 18 practical situations where incidents regularly occur. This is a set of difficult operational situations that need specific attention to do the work right. They can be used to increase understanding and competency and to deal with these complex situations safely.

Figure 16 EPSC Process Safety Fundamentals Pictograms

The process safety fundamentals differ from established "Life Saving Rules" that are more basic safety rules for everybody like "Buckle-up when driving". Process safety fundamentals are related to best practices in complex operational situations involving hazardous chemicals.

15.4 The Human Factor

A mistake from a single person can lead to a serious consequence incident (ref. Ludwigshafen 2016). Usually the person does not intent to make the mistake. It is important to identify the situations in which a single human error can result in a severe consequence. It is often related to multiple, sometimes confusing options, like identical pumps or reactors; multiple tanks; similar pipelines or flanges etc. Also procedures can be complex or not easy to follow. One cannot assume that an individual never makes a mistake, even when training and procedures are provided. An identification process can be applied that identifies critical manual situations. EPSC has performed a study on Human Performance to identify critical situations and define best practices to make critical work more clear.

15.5 Competency Management

Clear is that everybody must have the required knowledge and skills to work at a hazardous facility. This requires training and experience and a system to manage that. Typically roles and responsibilities are defined that include the required competencies. A training matrix can be used to validate all obtained their required training.

15.6 Contractor Management

As chemical operations work with contractors, they must be managed and protected from chemical hazards. The chemical operation must be protected against failures from contractor. The best strategy is to avoid that contractors operate or open equipment with chemicals or pressure. Experience demonstrates that this is difficult to manage. The following practices can help:

- Contractor work hazards are analysed and authorized by a Permit to Work system.
- Equipment can be isolated and cleaned with a stepwise isolation procedure that is verified and signed by operation.
- Lock, Tag and Try (LTT) or Lock-out, Tag-out, Try-out (LOTOTO) can help to assure equipment remains isolated, and kept free from chemicals.
- Contractors may think that they know the site well, but have started work on the wrong equipment. The only way to avoid this is to join the contractor in the field and do a field check at the location of the work. Identify with paint or field tags where the work needs to be done.
- Last Minute Risk Assessment (LMRA) to validate that preparation is complete, and the work in the field can start.

16. European Legislation

Europe (EU) has specific legislation on hazardous chemicals. It's goal is to protect people and the environment and also to create an equal playing field for European producers. European legislation is implemented into the member countries' legal systems, and can become more specific on the topic. Specific legislation to be mentioned are:

16.1 Seveso III legislation

When a production or storage location contains more chemicals than the threshold, the site becomes a Seveso site. This means it must comply with the Seveso legislation. This includes a description of the site, identification and evaluation of hazards, establishing safety concepts and safeguarding measures, and a management system. Authorities allow the site to operate according a permit, that states the terms and conditions. The site needs to be audited by the authorities to spot-check compliance.

An important feature and distinctive element of the Seveso regulation is the so-called safety case, which asks companies to identify the hazards and the safety measures, which control the risk, in an early phase as a part of the permitting process. This ensures a proactive stance in full view of the hazards, and a detailed plan to control the hazards. After each relevant plant change, the safety case is updated, and periodically the whole safety case is reviewed as part of the process of maintaining the permit. Besides the duties for the operating company, the safety case also ensures an active role of the regulator, including duties such as a yearly review visit.

16.2 Quantitative Risk Analysis - QRA

As part of the Seveso report, a QRA study is often included to determine how far the risk of the chemicals involved reaches. For this study, a specific software (like PHAST) may be used that assumes a certain leak size and calculates the outflow. From that calculation, the effects of a heat of a fire, the blast wave from an explosion, and the toxic cloud are estimated by the tool. The output from this is often presented as the likelihood contours for a single fatality.

Figure 17 Risk contour plot from QRA study, with single fatality probability rates. 10^{-6} means a person will die on average once per million years on that spot.

16.3 Pressure Equipment Directive - PED

When processing equipment is rated above 0.5 barg overpressure, the manufacturing and putting into market become part of the European legislation on pressure equipment. This specifies requirements on design, construction, checks / inspections, and documentation. For equipment with higher hazard potential, a "Notified Body" accredited by the state validates the design, performs a pressure test, and provides a "Conformité European" CE certificate that allows the equipment to be sold and used in Europe. Pressure equipment integrity in operation must be regularly validated during the lifetime of the equipment, by certified inspectors.

16.4 ATmosphères EXplosives - ATEX

ATEX stands for the French term "ATmosphères EXplosives", or explosive atmospheres in English. It has the goal to avoid explosions where flammable materials may be present. Therefore, chemicals that can create an explosive atmosphere have to be identified and, when above the threshold quantity, have to be managed by ATEX. The legislation distinguishes between explosive atmospheres created by gases from those created by dusts.

Identification of areas, where an explosive mixture could exist, is the responsibility of the owner of the process area. The legislation has three different zonings 0, 1, 2 for gasses and 20, 21, 22 for dust. They are based on the likelihood for the presence of an explosive mixture. The scope of ATEX is limited to leaks that can be expected as part of the operation, while major accidental releases are not included for the zoning. An Explosion Safety Document must be available, and the zoned areas must be indicated in the field. Making equipment that does not provide an ignition source is a responsibility of the equipment manufacturer. Such equipment needs to be CE certified when sold and used in zoned areas.

Figure 18 Triangle indicating ATEX zoned area and 6 corner (diamond) Equipment that can be used in a zoned area

16.5 Registration, Evaluation and Approval of Chemicals – REACH

Chemicals that are produced in, or imported into Europe need to be registered and evaluated. When approved, they can be sold and used under the conditions specified. The goal is to first understand all hazards before allowing chemicals on the market. The registration is done jointly by the manufacturers and importers and includes data of all potential hazards and methods for safe use.

16.6 Facility Siting

To increase the safety of personnel, it is good practice (not regulated by European legislation) to keep their offices at a safe distance from the hazardous chemical processes. To evaluate this, a so-called Occupied Building Risk Assessment (OBRA) can be carried out. Effect-distances of chemical incidents can be estimated and buildings for employees and contractors can be placed at a safe distance. When not possible to relocate the personnel outside the affected zone, a risk assessment can be done that includes the likelihood of the scenario. The contours generated by the QRA can be used to identify acceptable risk locations for buildings. Furthermore, technical measures, like a blast proof control room or gas tight escape rooms, can help to bring down the risk to an acceptable level.

17. Inherently Safe Design

"What you don't have, can't leak" is a famous phrase from Trevor Kletz. He promoted the principle of designing plants that are "Inherently Safe" or Safer. This can be best applied early in a project, since plant changes, such as implementing new technology in a later phase, might be difficult and expensive.

The inherent safe design works with the 4 guide words: “Eliminate” (the hazardous Chemicals), “Substitute” (for less hazardous materials or softer conditions), “Reduce” (quantities), “Simplify” (equipment or operation). Engineers can be trained and stimulated to use these principles, as they benefit safety for the lifetime of a plant.

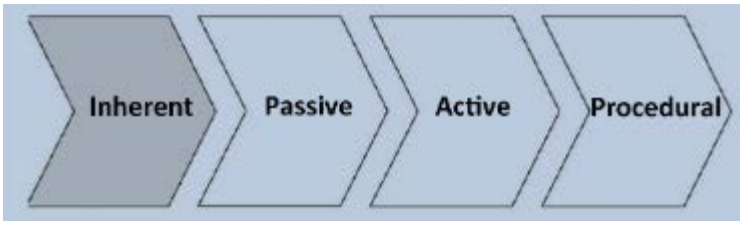


Figure 19 Process safety implementation order: Inherently Safe Design, followed by Passive barriers (Dike or Rupture Disk), Active barriers (electronic interlocks) and Operational Procedures (involving people)

18. Guidelines

Good design is essential for plants to make them safe. Helpful guidelines exist on specific equipment. EN and ISO norms, as well as American Petrochemical Industry (API) standards are often used in the chemical industry. Most European countries have useful guidelines and standards on specific chemicals and their use in processes, like for instance the use of ammonia in cooling units. Such guidelines can become mandatory when agreed in the environmental permit / permit to operate.
CEFIC facilitates European manufacturers of hazardous chemicals, to discuss on industry aspects like the safe use. Working groups exist on: Phosgene, Ethylene Oxide, Phenol, Petrochemicals, EuroChlor, Halogens, and others. These groups typically provide solid practical guidance on how to deal with the specific hazards of these chemicals during production, storage, use, and transport.

19. List of figures

20. Disclaimer

EPSC has provided this view on process safety free of charge. It is used to stimulate discussion on the practices applied to manage technical safety at facilities involving hazardous chemicals. The responsibility for consequences of the use of the content remains fully at the user. EPSC cannot be held liable for any consequences on the use of the content of this booklet.