PROCESS SAFETY

Table of Contents

Page

List of Figures

1.0 SCOPE

Process safety is a structured approach to managing the hazards inherent in processes by applying good design, engineering, and operating practices. The concepts of process safety are interrelated and were historically developed for the chemical process industries before being adopted by various regulatory agencies. As process safety concepts and practices have evolved, they have proven beneficial when applied in facilities with significant risks, that are outside the chemical industry. The guidance in this data sheet can be applied when practicing these concepts to significantly reduce the overall risk of failure for equipment, systems, or processes.

The intent of this data sheet is to assist in evaluating and developing procedures and programs for process safety that are commensurate with the hazards, and that can minimize the risk of property damage and business interruption. It is not intended to meet process safety requirements as established by governmental or other organizations. All elements of safety and risk that a facility must evaluate are not necessarily considered by this data sheet.

1.1 Hazards

In the high-hazard industries (e.g., power generation, chemical, mining) any losses that occur are typically the result of a breakdown in processes leading to a subsequent release of stored energy or materials, including ignitable liquid, flammable gas, and hazardous or toxic chemicals. Such losses result in significant property damage and extended loss of production or associated business interruption. Because of the hazards involved in these occupancies, a comprehensive process safety program commensurate with the hazards present is needed. Process safety programs provide a structured approach, consisting of several interrelated elements to identify, prevent, and mitigate these hazards.

1.2 Changes

July 2018. Interim revision. Guidance on asset integrity was updated to be consistent with revised FM Global Data Sheet 9-0, *Asset Integrity.*

2.0 LOSS PREVENTION RECOMMENDATIONS

2.1 Human Element

2.1.1 Management Commitment

Management commitment is the cornerstone of any successful program within an industrial facility. Without strong management commitment to process safety, well-intentioned programs can become neglected or eroded by outside forces (such as the pressure to produce). Strong management commitment ensures that all areas of process safety receive the necessary consideration, funding, and staffing.

2.1.1.1 Ensure a process safety program is in place. The key elements of a process safety program include the following:

A. A policy statement that clearly communicates the intent of the program to all sectors of the organization as well as outside contractors.

B. Accountability and assignments of responsibilities, along with consequences for failing to observe them.

C. Compliance with regulations and standards.

D. Metrics and audits, including key performance indicators (KPIs), trending of incidents, and loss lessons.

E. A system for certification of personnel in specific process safety roles.

F. Regular reviews to update the program to reflect changes in personnel, company position, or operations.

2.1.1.2 Ensure mangement support the process safety management program via employee empowerment, workplace participation, availability of operational resources, etc.

2.1.1.3 Establish a system for periodic auditing of the entire process safety management system.

2.1.2 Process Knowledge

2.1.2.1 Ensure all information compiled to understand the hazards and ensure the safe and reliable operation of the plant is available to all company personnel. This includes all information required to complete a process hazard analysis. Key elements include the following:

- Engineering drawings and calculations
- Process flow diagrams, piping & instrumentation diagrams (P&ID)
- Specifications for design, fabrication, and installation of fixed and rotating equipment
- Information on hazardous materials, including physical properties, safety data sheets (SDS) and maximum intended inventory
- Electrical classification
- Critical utilities and support systems
- Relief system design and design basis
- Safety systems design basis and capabilities
- Safe operating limits (SOL) and integrity operating windows (IOW) for operating parameters
- Consequences of deviation from these control limits
- Production chemistry, including mass and energy balances as well as reaction kinetics
- Thermal stability and reactive chemical hazards, including chemical and material compatabilities

Retain the information in a safe and secure location with appropriate document control. This may include an off-site location.

2.1.3 Process Hazard Analysis (PHA)

Originating in the chemical industry, a process hazard analysis (PHA) is a systematic approach for the identification, evaluation and control of hazards associated with a process. The intent of a PHA is to determine the potential causes and consequences of events (e.g. fires, explosions releases of hazardous chemicals) and evaluate factors which may affect the process. By doing a PHA, failure points, methods of operations and other contributing factors that can potentially lead to accidents can be identified and mitigated.

PHA's are now a routine tool used by a wide range of industries to identify and mitigate hazards applicable to a wide range of processes and equipment that could adversely affect their operations, personnel or environment.

2.1.3.1 Perform a process hazard analysis (PHA) on any processes using a recognized methodology such as, but not limited to, the following:

- Hazard and operability analysis (HAZOP)
- What-if
- What-if/checklist
- Failure modes effect analysis (FMEA)

In the PHA, consider the following:

- Routine and non-routine operating parameters, including the following:
  - Start-up and shut-down
  - Process deviations
  - Maintenance turnarounds
  - Utility failures
  - Control failures
  - Bypasses

- Processes that are regulated/not regulated
- Alternate modes of operations (e.g., decoking, recycle)
- Procedural changes and human factors

See Appendix C for common methodologies used in industry for performing PHA.

2.1.3.2 Create a PHA team consisting of trained personnel with cross-functional expertise. This typically includes engineering, operations, maintenance, safety, and other disciplines as needed. Ensure you have a competent facilitator formally trained in the particular PHA methodology to lead the PHA team.

2.1.3.3 Conduct periodic reviews that are commensurate with the risk, with an interval between reviews not to exceed 5 years.

2.1.3.4 Develop a system to prioritise and address PHA findings. Track all findings to resolution within an appropriate timeframe that is defined by the organization's PHA policy.

2.1.3.5 Identify critical utilities and develop load-shedding procedures to allow for the controlled shutdown of critical processes in the event of an emergency.

2.1.4 Asset Integrity

Effective asset integrity programs verify that the mechanical, electrical, pressure equipment and associated systems are adequately designed, installed, operated, maintained, and protected for the intended service. This management system uses operational and inspection data to ensure integrity and reliability throughout the service life of the equipment, reducing the likelihood of equipment breakdown and keeping energy sources contained.

2.1.4.1 Develop an Asset Integrity program in accordance with the guidance presented in FM Data Sheet 9-0, *Asset Integrity*, and Data Sheet 12-2, *Vessels and Piping* for equipment damage mechanism guidance to ensure asset integrity and reliability throughout the equipment service life.

2.1.4.2 Develop an Inspection, Testing and Maintenance (ITM) program at the core of the asset integrity program to monitor equipment conditions based on the identified process hazards and associated damage mechanisms and failure modes.

2.1.5 Management of Change (MOC)

The purpose of a management of change process is to prevent introducing unrecognized hazards during a change. This includes evaluating every change to technology, facilities or personnel at the earliest possible stage for its potential impact. Any change from original design intent represents a deviation. If the impact of this deviation is not fully understood, the change, even if minor, can cause a significant incident.

2.1.5.1 Develop a management of change (MOC) program that includes the following elements:

A. Formal, documented procedures to manage change in processes, equipment, technology, protection, facilities, and personnel.

B. Review and approval by competent supervisors/management of all system changes, permanent or temporary. Identify the personnel and/or departments responsible for reviewing and approving changes. Using a single reviewer for simple changes is acceptable, but large, complicated changes require a more complex process.

C. A method for identification and tracking of changes that are subject to the MOC procedures. Separate forms can be created for documenting change requests and approvals, as well as different types of changes to streamline the review and approval process.

D. Documentation of the process and mechanical design basis for proposed changes. The change request should clearly identify what the change is and the technical basis for the change.

E. Review of potential hazards associated with the change using an appropriate hazard analysis methodology, including the effects of the proposed change on upstream and/or downstream facilities, processes, and equipment.

F. Determination of the maximum allowable duration for any temporary or emergency change. Provide means for tracking the duration of such changes. Changes that go beyond the maximum allowable duration need to be revalidated following the normal MOC process.

G. Establishment of an administrative control system (e.g., a log, use of tags) for the control and tracking of jumpers, forces, and temporary modifications of safety and control systems. A hazard review and management signoff should be included as part of this system.

H. Identification, tracking, and monitoring of temporary modifications and repairs, including leak clamps. Appropriate inspection, testing, and maintenance programs should also be in place.

2.1.5.2 Establish relevant administrative procedures (e.g., documentation and/or checklists that cover hazards, records of personnel skills, responsibilities and training). Provide clear communication of the change and the consequences of that change to affected personnel such as maintenance engineers, operators, safety, and emergency response staff.

2.1.5.3 Post-change, finalize modifications to the operating procedures, P&IDs, asset integrity program, personnel training, etc. as needed.

2.1.5.4 Perform a pre-startup safety review (PSSR) prior to use of the system/process components for new or modified facilities whenever the modification is significant enough to require a change in the process safety information. This includes ensuring all recommendations developed during the MOC process have been addressed. Confirm all updates to operating procedures, personnel training, diagrams, drawings, etc. that may have been required as part of the MOC process have been completed prior to commissioning. Conduct the PSSR prior to introducing chemicals and/or energy into the process. Final documentation may be created post startup.

2.1.6 Incident Investigation

Failures in process safety programs often result in incidents and near misses. To fully understand what went wrong and how to prevent reocurrences, a comprehensive incident investigation program must be in place.

2.1.6.1 Establish an incident investigation program. Include the following elements:

A. A formal process for investigating incidents and near misses.

B. An investigation team with appropriate expertise (i.e., relevant operational, maintenance, and engineering expertice) led by a trained incident investigator.

C. A formal methodology to guide the investigative process (e.g., root cause analysis [RCA]). Establish benchmarks to ensure the timely completion of tasks.

D. Document all recommendations and develop a process to ensure completion of the recommendation.

E. Share the findings with all applicable members of the organization.

F. Incident trending: Use trending incident data for the identification and correction of recurring incidents, including reviews in the process hazard analysis.

Include and encourage, as part of the formal process, reports of all unusual occurrences to determine whether an incident has occured. Establish a simple process for prompt reporting, with training provided to employees on what should be reported.

2.1.7 Contractor Management

2.1.7.1 Establish a policy and programs to supervise contractors while they are at the facility.

2.1.7.2 Refer to FM Data Sheet 10-4, *Contractor Management,* for guidance in developing an effective program to manage contractors.

2.1.8 Operators

2.1.8.1 Establish operator training programs in accordance with FM Data Sheet 10-8, *Operators.* Include the following aspects:

A. The hazards of the materials and equipment used in the process.

B. The plant’s procedures for jumpers, forces, and temporary modifications of control systems.

C. Scenarios that involve potential variances from normal operation, including the worst-case scenario.

D. Understand standard operating procedures (SOP), alarm management, and emergency operating procedures (EOP). Additional guidance is provided in Data Sheet 10-8, *Operators,* including guidance for permit to work (PTW) systems.

3.0 SUPPORT FOR RECOMMENDATIONS

3.1 Background Information

3.1.1 Management Commitment

Management commitment is critical to the success of any process safety program and defines the safety culture for any company. It is important to have process safety engrained throughout the organization. This includes commitment within all levels of operations and management.

The lack of process safety programs and a management commitment to process pafety has been instrumental in some of the largest industrial losses in history. Several of the losses described in Section 3.2 were the result of fundamental breakdowns in management commitment and were instrumental in the development of process safety standards and regulations around the world.

3.1.2 Process Knowledge

Process knowledge, in general terms, includes both process safety information and the ability to understand and interpret the information.This is achieved by acquiring process information and using this knowledge while conducting process hazard analyses. It also includes the tracking and storing of key initial design bases, records of critical design decisions, design standards, site and equipment drawings, accident investigation information, etc. This data can be used as a baseline for future changes.

Data on process hazards and material properties can be obtained from numerous sources, including testing, manufacturer-issued safety data sheets (or equivalents), and literature sources.

The collection of data will preserve initial design records (to ensure that replacements comply with design intent), reasons for key design decisions (aid to future projects and modifications) and provide a basis for understanding how the process can be operated. It also serves as a baseline for evaluating future changes.

3.1.2.1 Example

A pharmaceutical company is proposing a new process using ignitable solvents, reactants, and catalysts to produce a intermediate material. The process will include a potentially exothermic reaction, mixing, distillation, and drying to produce a powdered product. The material is unique, and no known data on its properties can be found by conventional literature search.

Prior to conducting a PHA or determining levels of protection, the company needs to collect information on the process, materials, and equipment. Applicable codes, regulations, and standards used in the process may also require additional information to be collected. Such information may include the following:

A. Properties of all materials used in the process (raw, intermediate, and finshed), including the following:

1. Quantity
2. Physical state
3. Flammability limits
4. Incompatibilities
5. Corrosivity
6. Toxicity, including exposure limits

B. Dust characteristics

1. Particle size
2. Kst
3. Minimum Ignition Energy
4. Pmax

C. Reactivity and thermal stability

1. Basic chemistry
2. Physical properties
3. Runaway reactions
4. Thermal stability of potentially unstable materials
5. Specific testing may be required for unique materials
6. Material and energy balances
7. Consequences of deviation

D. Process information

1. Process description/overview
2. Process flow (e.g., block flow diagrams)
3. P&IDs
4. Utilities and support systems
5. Interlocks and safe limits
6. Operating procedures
7. Instrumentation and system design

E. Equipment information

1. Equipment design specifications, including anticipated damage mechanisms and failure modes
2. SOLs and IOWs for the operating parameters
3. Pressure relief valve sizing and design information
4. Equipment specific safety devices and interlocks

F. If this is a revalidation of a PHA, other considerations may include the following:

1. Outstanding recommendation from previous audits
2. Previous incident investigation reports
3. Previous PHAs conducted on the process
4. Previous MOCs

This information is needed prior to conducting the PHA and is to be maintained and updated as new information is learned. Over the life of the facility, new technology in process operation, inherent safety, or loss prevention techniques may be developed. While not known or cost-effective during initial plant design, they may become so later in the life of the facility. It is important for an organization to stay fully abreast of new technology and apply it as appropriate.

3.1.3 Process Hazard Analysis (PHA)

3.1.3.1 A PHA is performed to identify all potential risk of operating a process and to evaluate the mitigating measures to reduce the risk. The general process of the PHA is to identify deviations from normal operations, and what is the potential consequence of those deviations. The severity of the event along with the frequency of occurrence, defines the total risk.

The PHA then evaluates the mitigating measures in place and makes recommendations for improvements as needed. For complex processes, particularly with chemical reactions, the PHA may be a rigorous methodology and involve numerical calculations to determine likelihood. For simpler processes the PHA may be a less formal, with team member judgment on risk and adequacy of protection.

It is important to consider non-routine modes of operation during the PHA. Examples of non-routine modes of operation that require consideration include the following:

- Startup
- Shutdown
- Emergency shutdown
- Process recycle mode (putting the plant in hold mode)
- De-coking of furnaces
- Batch reactions
- Crusher bearing changes
- Turbine overspeed testing
- Battery overload and capacity testing

To illustrate why these are important, frequently startups require bypassing control and possibly safety devices until conditions are in normal ranges and the interlock can be satisfied and reinstated. In this case, the PHA must consider the risk while these devices are bypassed.

PHAs conducted during the early stages of a project, whether greenfield or expansion of an existing facility, can identify improvements to incorporate into the project. Often a preliminary PHA is conducted with the technology licenser or engineering firm, then a final PHA is done based on as-built conditions. See Appendix C for common PHA methodologies used in industry.

Common items for all methodologies:

A. Determine risk tolerance.

B. Gather and verify relevant process information. This can include all items from the process knowledge, MOCs, and recommendations from incident investigations.

C. Assess potential consequences.

D. Determine frequency of initiating event.

E. Identify protection measures in place

F. Create action items to improve risk.

G. Track all action items to closure.

The total risk (frequency and severity), as well as a company's risk tolerance, are frequently defined using a risk matrix. In such a matrix, frequency is on one axis and severity is on the other. Common matrices (see Figure 1) are 4x4 or 5x5; however, risk matrices can be any size.

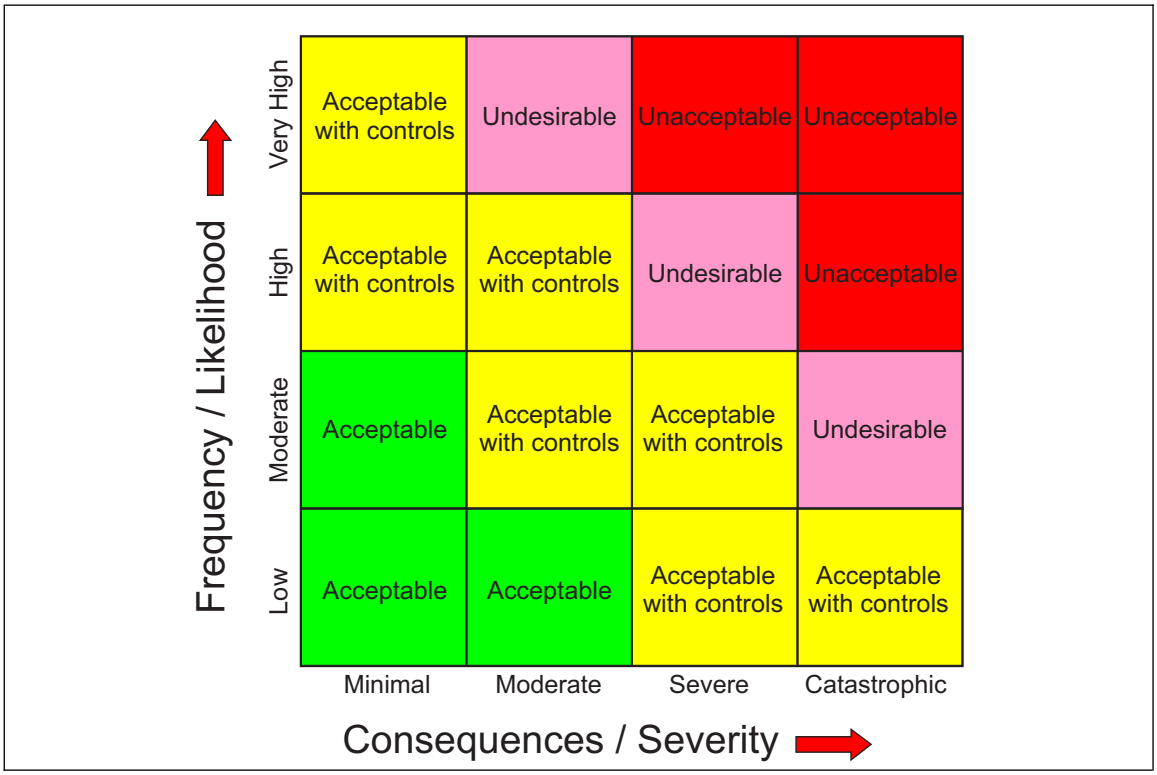

Fig. 1. Example of a typical 4x4 risk matrix

The frequency is based on the initiating event. For example failure of a check valve results in reverse flow through a piping system. There is extensive published data on failure rates on specific types of equipment present that can be used as a starting point to determine the frequency. With the fact published data may

be taken from various pieces of equipment, and typically not corrected for specific installations, care needs to be taken when using it. Published data may be modified based on plant experience with site specific conditions.

The severity may be ranked based on the consequences on personnel, the environment, physical assets, lost revenue, and impact on product quality or plant reliability. Not all types of consequences need to be included in a risk matrix. A company will pre-determine what an unacceptable level of overall risk is. Measures must be in place to reduce the risk, by reducing the frequency and/or the severity of the event.

Measures to prevent or mitigate the severity of an event are usually evaluated based on independent layers of protection. Figure 2 provides a example of typical layers of protection seen in a facility. The independence of these layers is a key component of the evaluation. For example, a control system can open a vent valve to reduce pressure in a vessel. Operators could also operate this valve manually. This could only be considered a single protection layer as failure of one device (the valve) could result in vessel overpressure. A separate installed pressure relieve valve (PRV) would, however, be a separate layer.

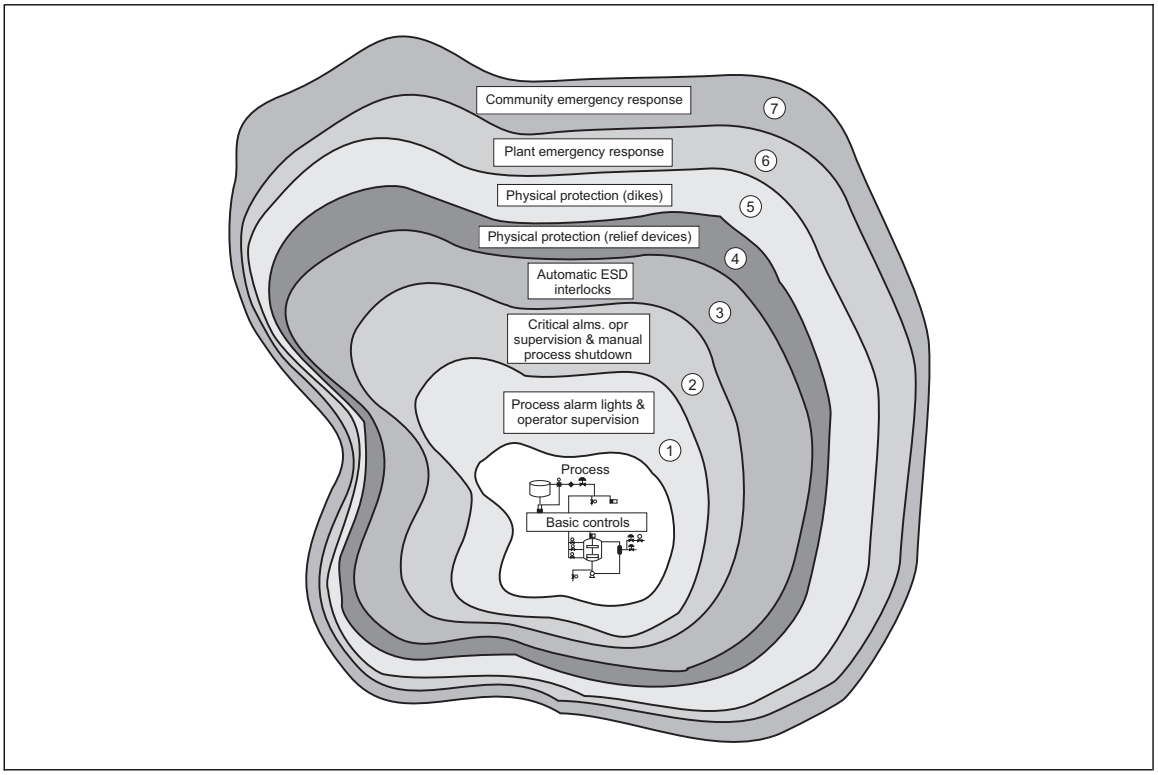

Fig. 2. Typical layers of protection

3.1.3.2 An experienced PHA team, both in terms of following the PHA methodology and the actual process is critical. By brain storming and relying on experience there is a high confidence that all hazards will be identified and accurate evaluation of protection completed, producing valuable recommendations for improvement. This does require that the team has expertise in the needed areas, has all needed information available and can access other resources for specific items that may be outside of their expertise.

3.1.3.3 Revalidation of the PHA is needed to ensure that process conditions and assumptions made during the PHA are still valid. Even with a comprehensive MOC program an accumulation of multiple changes over a period of years could result in an unrecognized risk.

3.1.3.4 The PHA will have findings. Management review of the findings and action items are assigned to responsible persons and include due dates. The action items are tracked until closure. Frequent review of the status are conducted, particularly focusing on items nearing the due date or overdue. A final review of the completed item is conducted to ensure that the intent of the PHA team was met and that the risk is effectively reduced.

3.1.4 Asset Integrity

An Asset Integrity program is a key element of process safety to help ensure the integrity and reliability of mechanical, electrical and pressure equipment as well as their associated systems. The integrity and reliability of the equipment takes into account the intended service of the equipment throughout its expected life cycle. Promoting integrity and reliability increases process efficiency and reduces equipment breakdown. Equipment breakdown is a leading cause of loss of containment leading to fire, explosion or other perils. Preventing equipment breakdown and keeping energy sources contained is contingent on how the equipment designed, installed, operated, maintained and protected. Effective asset integrity programs verify the original design by detecting, monitoring and trending the anticipated damage mechanisms. These programs are flexible to manage change in the process as well as operating conditions and parameters to align the ITM program. Full integration of asset integrity into the process safety program is the goal. Detailed guidance on the development of an Asset Integrity program is found in FM Data Sheet 9-0, *Asset Integrity*.

3.1.5 Management of Change

Management of change (MOC) means evaluating all changes except replacement-in-kind (RIK). This includes changes to technology, facilities, or personnel at the earliest possible stage for their potential impact on property loss prevention. The MOC element includes a review and authorization process for evaluating proposed adjustments to facility design, operations, organization, or activities prior to implementation to make certain that no unforeseen new hazards are introduced and that the risk of existing hazards not unknowingly increased.

Replacement-In-Kind for changes in facilities is the exchange or replacement of one piece of equipment or component that meets all of the original design specifications exactly with no deviations, (size, pressure rating, temperature rating, flow rating, metallurgy, etc.) and these would not be considered a change and require completion of the MOC process.

It also includes steps to help ensure that potentially affected personnel are notified of the change and that pertinent documents, such as procedures, process safety knowledge, and other key information, are kept up-to-date.

A written procedure is needed to define what a change is, how it will be requested, reviewed and approved, and implemented. Changes that should be managed can be as simple as replacing a valve with one of a different type or modifying an operating procedure. Complex changes can involve installation of new equipment or construction of a new plant.

3.1.5.1 Categories of Change

3.1.5.1.1 Changes in Technology/Process

Changes in technology/process arise whenever the process or mechanical design is altered. Typical instances include the following:

A. Changes in feedstocks, catalysts, product specifications, byproducts or waste products, fuels, equipment, design inventory levels, or materials of construction.

B. Changes in facilities (including physical changes) that would not necessarily appear on drawings or piping and instrument diagrams (P&ID). Examples:

1. Temporary connections
2. Replaced components that are “not in kind”
3. Transient storage
4. Temporary structures, piping, connections, hoses, or wiring
5. Temporary utility connections (steam, power, water, etc.)
6. Temporary software configurations, jumpers, shortened algorithms, bypassed controls
7. An alternative supply of process materials, catalysts, or reactants, such as through drums or tanks, temporarily located within the facility

C. Changes in operating procedures, including procedures for startup, normal shutdown, and emergency shutdown

D. Significant changes in operating conditions, including pressures, temperatures, flow rates, or process conditions different from those in the original process or mechanical design (i.e., outside the safe operating limit defined in the standard operating procedures)

E. Bypass connections around equipment that is normally in service

F. Changes to the control systems, including changes in alarms, instrumentation, and control schemes

G. Corrective actions developed as a result of incident investigation

H. Changes made in the process or mechanical design or in operating procedures that result from a PHA performed

I. Modifications to the process or equipment that cause changes in the facility's asset integrity program

J. Modifications to the process or equipment that cause changes in the facility's relief requirements

K. Modifications to protection systems, including fire protection

L. Modifications to the process or equipment that cause changes in the facility's protection requirements, including:

1. Fire pump
2. Water supply
3. Fire protection systems (sprinklers, special protection)
4. Drainage and containment

3.1.5.1.2 Changes in Personnel or Organization

Changes in personnel or organization are those in which key responsibilities are affected (e.g., retirement, promotion, sickness, death, leave-of-absence). These changes might cause a lapse in continuity of responsibility. Examples include the following:

A. Changes in staffing levels

B. Staff experience

C. Use of outside contractors

D. Personnel changes within a department or to another department

E. New personnel being assigned to a position for the first time

F. Changes in the duration of shift schedules affecting the human factor element of process safety

G. Policy changes (e.g., a significant cut in a maintenance department's budget) that could require an employer to alter its mechanical integrity procedures concerning the timeliness or frequency of tests, inspections, repairs, or replacements

3.1.5.1.3 Duration of Change

Changes are usually defined as permanent, temporary, or emergency.

A. Permanent change: A change that involves a permanent modification to the facility, technology, or personnel. An advance review of the proposed change is needed following the normal management of change (MOC) process.

B. Temporary change: A change that is not intended to be permanent, instead having a predetermined termination date and time. An advance review of the proposed change is needed following the normal management of change (MOC) process.

C. Emergency change: A change that must be made to maintain or resume safe operations (e.g., a plant breakdown or shutdown occurring on off-shifts or weekends). Such changes require a formal evaluation approval process although this process is often expedited. Additional safeguards might be implemented for the duration of the change (e.g., frequent monitoring).

Identifying what constitutes a change and where changes might originate, are important for an MOC system to be able to address all potentially significant change situations. This can include requests for changes that are made by operations, maintenance, engineering, or procurement.

There may be occasions when action items are occasionally deferred based on the lower risk they pose until after startup (e.g., the installation of heat tracing on bypass piping commissioned in summertime). While not as critical as larger, more complex changes, these are still changes that need to be tracked to completion in a similar manner.

3.1.5.2 Forces, Jumpers, and Temporary Modifications of Safety Control Systems

There are ways to impair or bypass safety systems. Overrides or impairments can take various forms, such as forces or jumpers.

A “force” is a controlled output that is unchanged by input or feedback in a control loop. It is designed to ensure a certain output (control signal, set point signal, or other output) that will not be affected by otherwise related feedback and inputs from the system.

A “jumper” is similar to a force, but relies on physically bypassing a device.

Both forces and jumpers are changes and are covered under an MOC program. In practice, however, these are typically managed using a separate system. Important aspects of this program are hazard evaluation, notification of all affected operators, contingency plans to reduce the risk, and formalized plans to complete repairs.

3.1.5.3 Leak Clamps

Installing leak clamps on piping or vessels is a change to the process equipment and should be completed using the MOC program. Similar to forces, this is frequently handled through a separate program specific to leak clamps.

The important aspects of the program are a hazard evaluation based on the level of risk, and verification that the clamp is suitable for the service. This can include engineering the clamp and verifying the integrity of the piping or vessel where the clamp is to be positioned. The location of the clamps should be documented and plans on when to remove the clamp and complete permanent repairs formalized. Typically this is completed at the next available maintenance opportunity, such as a turnaround.

3.1.5.4 Pre-Startup Safety Reviews (PSSR)

Typically conducted in conjunction with the management of change (MOC) procedure, a PSSR is performed for new facilities and when significant modifications are made.

PSSRs can be physical walkthroughs that are designed to identify incomplete changes, that could present a potential safety hazards before operating the process. This then allows these identified deficiencies to be corrected before the process is started.

Pre-startup safety reviews should also be conducted prior to commissioning and/or putting into service any new, significantly modified or previously mothballed processes or equipment.

3.1.6 Incident Investigation

Incidents can be grouped many ways, but the three general types listed below will serve for most purposes.

A. Major accident: An incident in which the impact is above an acceptable level, usually involving major property damage, extended business interruption, significant spills, and/or multiple injuries or fatalities.

B. Accident: An incident having an undesirable impact on company resources, usually involving minor property damage or a single injury.

C. Near-miss: An incident with the potential to be an accident or major accident.

The depth of investigation is commensurate with the level of complexity and size of incident. Less-formal investigations or simply trending of the incident data may be applicable for small events or those that happen more frequently (e.g., a broken handrail). In these cases, the incident investigation may be completed by qualified individuals or a small team of qualified personnel (e.g., a broken handrail merely requires the incident to be logged and subsequently corrected).

In the event of larger incidents, such as an explosion, loss of containment, or fire, a full incident investigation requiring a large team of qualified members may be needed.

The purpose of incident investigation is to prevent recurrence. This requires a management system that achieves the following:

- Investigates incidents to determine the root cause.
- Develops recommendations to prevent a recurrence.
- Ensures follow-up to complete recommendations as part of MOC.

3.1.6.1 Basic Elements for Full Incident Investigation Programs

A. In order to conduct a thorough investigation, a qualified person or team of people needs to be assembled to determine and analyze the facts of the incident. Appropriate investigative techniques and methodologies are then used to reveal the underlying root cause.

B. Determining the cause (root cause and contributing causes) is one of the main functions of the incident investigation team. Some special effort will likely be needed to determine underlying system-related causes. Training or lack of training is rarely a root cause but often a symptom of another problem. Issues such as poor design, incorrect installation, faulty maintenance, inadequate procedures, and bad management decisions are all factors that can cause or contribute to situations that are inherited by operators, rather than operators being the main cause of an accident.

C. The team then generates a report detailing facts, findings, and recommendations. Typically, recommendations are written to reduce risk by improving the process technology, upgrading the operating or maintenance procedures or practices, and upgrading the management systems.

D. The report is shared with all applicable members of the organization.

E. After the investigation is completed and the findings and recommendations are issued in the report, good practice is to have a system in place to implement these recommendations. This is not part of the investigation itself, but rather the follow-up related to it. It is not enough to put a technological, procedural, or administrative response into effect. Periodic monitoring of the action for effectiveness is also valuable which then allows, where appropriate, modification of the action meet the intent of the original recommendation.

The extent of the investigation required is typically based on the a management review of the initial incident report and the classification criteria. Small events, therefore, may not require a full formal investigation as they may have no significant potential consequences to property damage or business interruption. The use of metrics keep track of and trend the number and type of small occurrences can be helpful in this process.

3.1.6.2 Investigative Techniques and Trending

The following are the three key components needed to ensure effective incident investigation and identification of root causes:

A. A description and schematic representation of the incident sequence and its contributing events and conditions

B. Identification of the critical events and conditions in the incident sequence

C. A systematic investigation into the root causes of the incident

When choosing a root cause analysis methodology, it is important to recognize that no single tool does everything. Good methodologies sometimes use combinations of tools. Care should be taken in choosing a methodology, depending on the existing culture within the organization, the investigation leaders, the level of training resources available, and the complexity of the incident.

It is important to understand that the various tools use different types of logic to arrive at a result. These types of logic are intuitive, deductive, inductive, or a combination.

Some of the common methodologies are:

- FTA: Fault Tree Analysis
- AAM: Accident Anatomy Method
- MORT: Management Oversight and Risk Tree

- MCSOII: Multiple-Cause Systems-Oriented Incident Investigation
- HAZOP: Hazard and Operability Analysis
- CELD: Cause and Effect Logic Diagram
- FMEA: Failure Mode and Effect Analysis
- 5-WHY: An interrogative technique to determine the root cause of a single defect or failure by asking the question “Why” five times

Trending the incidents helps to identify common links in the incident data. Trending provides information to allow precautions to be taken at the affected facility and other facilities, and apply lessons learned in future design. The team should be able to clearly focus on commonalities. The categories may include specific system deficiencies or breakdowns such as design, training, mechanical integrity, and specific hazard exposures.

3.2 Illustrative Losses

3.2.1 Chernobyl Nuclear Accident

In April 1986, a nuclear reactor in the USSR (modern day Ukraine) lost containment. The facility was attempting to test an emergency shutdown system (safety system) and, in the process, lost control of the reactor. The reactor core overheated, resulting in an explosion and loss of primary and emergency containment. The event resulted in 31 immediate fatalities and the relocation of over 500,000 people. The facility never restored operations and the surrounding region has been deemed uninhabitable. Including the direct costs of damage, resettlement, and ongoing mitigation expenses, the Chernobyl accident is generally considered the most costly industrial accident in history. Total estimated costs vary widely, but are widely recognized to be in excess of US$250 billion.

In the aftermath, an exhaustive incident investigation was completed. While there were a large number of findings, the following were the most relevant:

A. Operator error: The operators during the sequence of events leading up to the explosion increasingly deviated from the established operating procedures.

B. Safety systems: Key safety systems were disabled to allow for testing of the targeted system. This included the emergency core cooling system (ECCS). There was no contingency plan or consideration for what would happen if the test failed.

C. Design deficiencies: Following the event, new research revealed that the use of graphite-tipped moderators exacerbated the event in the initial shutdown phases.

The aggregate conclusion of the deficiencies was a fundamental failure of the management systems. This was one of the first events where the term deficient “safety culture” was used to describe the aggregation of the deficiencies.

3.2.2 Bhopal Gas Release

In December 1984, a pesticide manufacturing plant in India accidentally released a large quantity of methyl isocyanate (MIC). Over 500,000 people were exposed to the resulting toxic cloud, resulting in an official death toll of 3,787 people. Some unofficial estimates place the death toll at more than 20,000 people. This event is generally considered to be the most deadly industrial accident in modern history.

Incident investigations were conducted and the following are some of the findings:

A. Poor facility funding and operator training had resulted in degradation of the safety culture and a poor recognition of the hazards and risks associated with MIC.

B. Water was introduced into the MIC tank, resulting in an uncontrolled reaction and release through the emergency vent system.

C. Safety systems, including an emergency vent scrubber and flare, were out of service, allowing the cloud to be released directly to atmosphere.

D. Poor facility siting resulted in a large number of people living in very close proximity to the plant.

The aggregate conclusion of the findings was poor management systems and management commitment to safely operate this high-hazard facility.

3.2.3 Flixborough Caprolactam Plant Loss

On June 1, 1974, the Flixborough Works of Nypro (UK) Limited, experienced a massive vapor cloud explosion, killing several people onsite and causing injuries and property damage within a large area surrounding the plant.

The Flixborough process produced caprolactam, an intermediate in the production of nylon. Cyclohexane was partially oxidized, forming cyclohexanol and cyclohexanone, with the latter feeding the caprolactam process. Cyclohexane was recirculated through a series of six reactors in sequence. Each successive reactor was arranged at a lower elevation than the previous one, allowing the cyclohexane to flow by gravity from one reactor to the next. The reactors were interconnected by 28 in. (0.7 m) diameter lines with corrugated expansion bellows installed at the vessel outlet and inlet flanges.

Reactor 5 had been removed from service to allow needed repairs to be made. To permit continued operation, a temporary piping assembly was fabricated to bridge the gap between the outlet on reactor 4 and the inlet on reactor 6. Because of the elevation changes, the temporary pipe was not straight and had bends in it. The pipe's diameter was only 20 in., less than the normal 28 in. (0.7 m) interconnection. Bellows, also 28 in. (0.7 m), were installed between each reactor and the temporary pipe. The only support for the temporary pipe was the scaffolding on which it rested.

The temporary pipe performed satisfactorily for two months until a slight rise in the pressure occurred, causing the pipe to twist. The bending moment was strong enough to tear the bellows, releasing pressurized cyclohexane at 302°F (150°C). When the piping failed, an estimated 30-50 tons (27-45 tonnes) of cyclohexane vapor was released that resulted in a vapor cloud explosion. The explosion and subsequent fires totally destroyed the plant.

The lack of a systematic evaluation to consider the hazards and consequences of a modification/change is one of the primary lessons learned from this incident. Failure to recognize the need to restrain the pipe resulted in the failure of the bellows and the loss of containment of the material.

3.2.4 Failure on Startup of New Polyethylene Terephthalate (PET) Plant

Ethylene glycol is reacted with purified terephthalic acid (PTA) to produce PET resin in heated reactors. Hot acetic aldehyde vapor (a reaction by-product) are removed via contact with ethylene glycol inside scrubbers. Both the scrubbers and the reactors are heated with heat transfer fluid to facilitate their operation.

During startup of a new PET plant, a pump failed on a PET reactor. With no spare vessel available to transfer the contents into, and with the replacement of the pump deemed a simple fix, the contents of the reactor vessel were left in situ, heated to the normal reactor temperature of 536°F (280°C).

When the process was restarted, the scrubber for the process was found not to be in service. As circulation commenced, the temperature difference between the two fluids in the scrubber created an under-pressure situation in the scrubber unit, allowing external air to be drawn into the scrubber. A series of fireballs resulted in the scrubber area, damaging equipment nearby.

During construction of the unit, a nitrogen line designed to prevent air from the being drawn into the scrubber unit was not installed correctly. A PSSR completed prior to the startup of the process identified this nitrogen line as being present, but it was not shown on the P&ID. Although identified, the nitrogen line was deemed a deviation that need not be investigated until after startup was completed.

Completion of all action items on the PSSR would have prevented the unit from starting until the issues with the out-of-service scrubber and the nitrogen line were corrected. This would have prevented the loss.

4.0 REFERENCES

4.1 FM

Data Sheet 7-14, *Fire Protection for Chemical Plants*
Data Sheet 9-0, *Asset Integrity*
Data Sheet 10-1, *Pre-Incident Planning*
Data Sheet 10-4, *Contractor Management*
Data Sheet 10-8, *Operators*

4.2 Others

Bridges, William and Marshall, Mike. *Necessity of Performing Hazard Evaluations (PHAs) of Non-Normal Modes of Operations)* Startup, Shutdown and Online Maintenance). Mary Kay O'Conner Process Safety Center. 18th Annual International Symposium (October 27-29, 2015).

Center for Chemical Process Safety (CCPS). *Guidelines for Asset Integrity Management.* 1st edition. John Wiley & Sons, New York (2016).

Center for Chemical Process Safety (CCPS). *Guidelines for Hazard Evaluation Procedures.* 3rd edition. John Wiley & Sons, New York (2008).

Center for Chemical Process Safety (CCPS). *Guidelines for Risk Based Process Safety,* John Wiley & Sons, New York (2007).

Directive 2012/18/EU, 4 July 2012. Control of Major-Accident Hazards Involving Dangerous Substances - Seveso III (repeals Directive 96/82/EC -Seveso II).

Environmental Protection Agency. 40 CFR Part 68. *Accidental Release Prevention Requirements: Risk Management Programs Under Clean Air Act Section 112(r)7* (1996).
Environmental Protection Agency. 40 CFR Part 68. *Accidental Release Prevention Requirements: Risk Management Programs Under Clean Air Act Section 112(r)7 Amendments* (1999).

Occupational Safety and Health Administration (OSHA). OSHA Regulation 29 CFR 1910.119. *Process Safety Management of Highly Hazardous Chemicals.* August 26, 1992.

Occupational Safety and Health Administration (OSHA). www.osha.gov "Voluntary Protection Programs."

APPENDIX A GLOSSARY OF TERMS

ACC: American Chemical Council.

AIChE: American Institute of Chemical Engineers.

API: American Petroleum Institute.

ASME: American Society of Mechanical Engineers.

COMAH: Control of Major Accident Hazards.

Escalating event: Fire, explosion, equipment breakdown, or other negative impact that occurs after an initial cause or situation.

Ignitable liquid: Any liquid or liquid mixture that is capable of fueling a fire, including flammable liquid, combustible liquid, inflammable liquid, or any other term for a liquid that will burn. An ignitable liquid is one that has a fire point.

MHF: Major hazard facility

P&ID: Piping and instrument diagram.

PHA: Process hazards analysis

Process: A process is a systematic series of mechanical or chemical operations that produces or manufactures something. Processes are integral to industrial facilities and may consist of one or many systems within each process.

RAGAGEP: Recognized and generally accepted good engineering practice.

RBPS: Risk-based process safety. A formally established and documented set of activities designed to produce specific results in a consistent manner on a sustainable basis.

RMP: Risk management plan. A plan required for facilities under the Clean Air Act Amendments (1999) for the prevention and mitigation of accidental chemical releases of substances regulated under the Clean Air Act (1990).

APPENDIX B DOCUMENT REVISION HISTORY

July 2018. Interim revision. Guidance on asset integrity was updated to be consistent with revised FM Global Data Sheet 9-0, *Asset Integrity.*

April 2017. The entire data sheet was revised. The following major changes were made:

A. Changed the title of the data sheet from *Loss Prevention in Chemical Plants* to *Process Safety.*

B. Reorganized the document to provide a format that is consistent with other data sheets.

C. Redefined the scope of the data sheet to allow the application of process safety across all industries, commensurate with the hazards present.

D. Updated the terminology to bring the data sheet in line with current industry usage.

E. Added recommendations for areas of process safety that drive property losses and associated business interruption, including management commitment, process knowledge, process hazard analysis, asset integrity, management of change, contractor management, incident investigation, and operators.

F. Added support material on other process safety programs around the world.

G. Deleted the appendix on “Other Sources for Chemical Process Safety Guidelines.”

H. Added support material on the 20 Elements of Process Safety.

July 2015. Interim Revision. Minor editorial changes.

April 2013. Minore editorial changes were made.

January 2012. Terminology and guidance related to ignitable liquids has been revised to provide increased clarity and consistency with regard to FM Global’s loss prevention recommendations for ignitable liquid hazards.

Added text to section 2.1.3.1 about the need to evaluate ignitable liquid and combustible dust hazards even if inherent safe practices are being undertaken.

September 2010. Minor editorial changes were made for this revision.

June 2009. Reference to Data Sheet 7-53, *Liquefied Natural Gas (LNG)*, was deleted.

May 2008. Minor editorial changes were made.

September 2000. This revision of the document has been reorganized to provide a consistent format.

May 1999. Completely rewritten using PSM as basis.

February 1974. Original publication.

APPENDIX C COMMON PHA METHODOLOGIES

C.1 Checklist

A. Non-scenario-based hazard evaluation.

B. Uses a written list or steps in a procedure to generate questions based on the deficiencies seen.

C. Can be used to assess materials, procedures and equipment and typically is used to ensure compliance with codes and standards.

D. Easy to use and can be used at any stage in the lifetime of a process or operation.

E. Limited by the experience of the author of the checklist.

F. Can be completed by an individual.

C.2 What-If Analysis

A. Scenario-based hazard evaluation.

B. Can be used at every stage within the life cycle of a process/operation.

C. Brainstorming method that is conducted by a team.

D. Requires experienced and knowledgeable personnel.

E. Simple format that is easily facilitated and can be executed quickly.

C.3 What-If Analysis/Checklist

A. Scenario-based hazard evaluation.

B. More structured than the What-If Analysis method.

C. Combines the brainstorming team approach of the What-If analysis with the structured approach of the Checklist method.

D. May be used at any stage of the life cycle of a process/operation.

E. Checklist quality is dependent on the author of the checklist.

F. Works best with an experienced team.

G. Encourages deviations and consequences beyond the experience of the checklist authors to be considered to determine safeguards.

C.4 Hazard and Operability Study (HAZOP)

A. Scenario-based hazard evaluation.

B. Detailed and structured review of a process or operations using a systematic methodology.

C. Can be used for continuous or batch processes.

D. Uses and interdisciplinary team (usually 5-10 people).

E. Requires an experienced Team Leader who is trained in the HAZOP methodology.

F. Requires a method to track the issues that have been considered and the action items that are generated.

G. Can take several months to complete (for a medium sized plant)- making it difficult to perform the review as a continuus process over an extended time period.

C.5 Failure Mode and Effect Analysis (FMEA)

A. Scenario-based hazard evaluation.

B. Evaluates failure modes of equipment and their effect on a system or the plant.

C. Equipment focused.

D. Can be performed by a single individual with extensive review, but is more typically conducted by a team hwose members are experienced with the equipment, the failure modes and how these modes can potentially affect other systems are needed.

E. Each individual failure mode is independent and combinations of faults are not addressed.

F. Failure modes that result in safe operation are addressed in addition to those that contribute to a loss event.

G. Time and cost are in proportion with the size and complexity of the equipment being examined.

C.6 Fault Tree Analysis

A. Scenario-based hazard evaluation.

B. Deductive technique focusing on the event and then working backwards to determine the cause of that event.

C. Well suited for analysis of systems that have a high level of redundancy present.

D. Often used in conjunction with other methods (e.g. HAZOP) where are more detailed analysis is required.

E. Individual or team approach can be used for this method. Experienced and knowledgeable personnel are required throughout the analysis process.

Time and costs associated with PHA methodologies are dependent on the complexity of the operation/process being analyzed and the level of resolution needed.

APPENDIX D CODES AND STANDARDS RELATING TO PROCESS SAFETY

The most well-known mandatory codes are those in the United States and the European Union. Direct adoption of these codes is not uncommon, especially in the Asia-Pacific region. Other countries will use these regulations as a framework, adapting them to local needs. The following information is for general information purposes. If more information is desired, refer to the applicable country's standard.

D.1 European Union (EU)

The applicable standard in the European Union is Directive 2012/18/EU *The Control of Major Accident Hazards involving Dangerous Chemicals (aka Seveso III*).

A. The directives contain the following key provisions:

1. Unifying standards across the European Community

2. Identification of competent oversight authorities

3. Provision of a framework of controls involving identification, assessment, control, and mitigation

4. Information exchange between member states and the European Community

5. Community-wide reporting, with database, of major accidents

B. Key components include the following:

1. Classification of a facility based on threshold quantities of a material. Facilities can be either classified as an Upper Tier location or a Lower Tier location.

2. Development of a Major Accident Prevention Policy (MAPP). The MAPP must include the development of a safety management system that includes the following aspects, "proportionate to the major accident hazards:"

a. Organization and Personnel

b. Identification of Major Hazards

c. Operations Control

d. Management of Change

e. Planning for Emergencies

f. Monitoring Performance

g. Audit and Review

3. For Upper Tier facilities, the development and filing of a Safety Report with the relevant authorities is mandatory. The Safety Report should demonstrate that the MAPP and the associated safety management system have been put into effect and that major accident hazards have been identified and controlled.

4. To demonstrate that “all measures necessary” have been taken to prevent or mitigate the effect of a major accident. This has been interpreted as reducing risks to a level that is “as low as reasonably practical” (ALARP). To achieve ALARP, it is implied that some form of risk assessment have been completed to assess the level of the risk and then determine whether the costs necessary to implement risk improvement are justified against the benefits of that risk reduction.

5. Inspections by Member States (i.e. government audits). These are compulsory on the states and companies in the EU.

D.2 United States (USA)

D.2.1 Occupational Safety and Health Administration (OSHA)

OSHA’s process safety regulations, “Process Safety Management of Highly Hazardous Chemicals” (29 CFR 1910.119) apply to “any activity involving a highly hazardous chemical including using, storing, manufacturing, handling, or moving such chemicals at the site, or any combination of these activities.” Highly hazardous chemicals are listed in the OSHA regulations and have a threshold quantity associated with them. If a hazardous chemical exceeds the threshold quantity given, then the OSHA regulations apply.

In addition the OSHA regulations also apply to processes handling in excess of 10,000 lb (4535.9 kg) of a “flammable liquid with a flashpoint below 100°F (37.8°C) on site in one location.”

Under the OSHA regulations there are 14 process safety elements that form the regulations:

- Process Safety Information
- Process Hazard Analysis
- Operating Procedures
- Training
- Contractors
- Mechanical Integrity
- Hot Work
- Management of Change
- Incident Investigation
- Compliance Audits
- Trade Secrets
- Employee Participation
- Pre-startup Safety Review
- Emergency Planning and Response

D.2.2 OSHA Voluntary Protection Programs (VPP)

Starting in 1982, the Voluntary Protection Programs (VPP) are an OSHA initiative to promote safety and health in the workplace. Sites are invited by OSHA to participate in the program, where they must adhere to and be assessed against, performance-based criteria covering occupational health and safety management systems. Those that qualify are awarded a recognition at one of three levels based on their achievements in the prevention and control of occupational health and safety hazards within their workplace.

D.2.3 Environmental Protection Agency (EPA) Risk Management Plan (RMP)

This program (EPA 40 CFR 68) has a similar framework to the OSHA regulations with the primary objective being to prevent an accidental offsite release.

Organisations are required to develop a report to the EPA, which includes worst-case release scenarios, amongst other things. Many of the elements of RMP are similar to those in the OSHA regulations and are functionally administered in the same onsite program.

D.3 Voluntary Process Safety Programs

D.3.1 Responsible Care®

The Responsible Care program started in Canada in 1985 and is a voluntary initiative that currently operates in over 60 countries around the world.

The program expanded in 2006, with the development of the Responsible Care Global Charter, to provide commonality between all members.

Members agree to follow several foundational principles, involving continuous improvement of their environmental, health, and safety knowledge and systems; communication with stakeholders (e.g., customers and employees); and working with authorities to assist in the development and implementation of improved standards and regulations.

Companies that wish to become members of the American Chemical Council (ACC) must sign the Responsible Care charter in order to become an ACC member.

D.3.2 Center for Chemical Process Safety

The Center for Chemical Process Safety (CCPS) is a not-for-profit corporate membership organization within the American Institute of Chemical Engineers (AIChE). CCPS's main focus is to develop and share technical information to assist in the prevention of major chemical accidents.

CCSP created a set of risk-based process safety (RBPS) guidelines in conjunction with their member companies and several global process safety specialists. These guidelines are considered a "best practice" approach in the field of process safety. The CCPS guidelines assume that not all risks and hazards are equal, and therefore the focus should be on the more significant hazards and higher risks. The guidelines do not define which processes require process safety oversight; rather they are intended to be applied by users according to their needs.

The CCPS guidelines are made up of four foundational pillars, which are then divided into twenty (20) elements:

A. Commit to process safety

- Process Safety Culture
- Compliance with Standards
- Process Safety Competency
- Workforce Involvement
- Stakeholder Outreach

B. Understand Hazards and Risk

- Process knowledge management
- Hazard Identification and Risk Analysis

C. Manage Risk

- Operating Procedures
- SafeWork Pracices
- Asset Integrity and Reliability
- Contracor Management
- Training and Performance Assurance
- Management of Change
- Operational Readiness
- Conduct of Operations
- Emergency Management

D. Learn from Experience

- Incident Investigation

- Measurement and Metrics
- Auditing
- Management Review and Continuous Improvement

D.3.2.1 The 20 Elements of the CCPS Guidelines

Process Safety Culture

Process safety culture is defined as “the combination of group values and behaviours that determine the manner in which process safety is managed.” A plant with a strong process safety culture will typically have established process safety as a core value, and this will backed by strong leadership at all levels of the organization. They will also possess high standards of performance that are enforced, open communications across all levels and a timely response to process safety concerns.

Compliance with Standards

Identifying and addressing relevant process safety standards, codes, regulations, and laws over the life of the process. These can be external or internal standards or national and international codes, along with local, state, and federal laws.

Process Safety Competency

Process safety competency is comprised of three interrelated actions:

1. Continuously improving knowledge and competency
2. Ensuring appropriate information is available to those that need it
3. Consistently applying what has been learned.

Workforce Involvement

This element provides a system for personnel at all levels within an organization to be actively involved in the design, development, implementation, and continuous improvement of the RBPS management system. Workforce involvement helps to ensure consistent implementation of process safety practices across a facility, along with ensuring competent personnel are involved in the development of all process safety practices and procedures.

Stakeholders Outreach

Stakeholder outreach involves the following:

1. Seeking out individuals or organizations that can be, or believe they can be, affected by company operations and engaging them in a dialogue about process safety.
2. Establishing a relationship with community organizations, other companies and professional groups, and local, state, and federal authorities.
3. Providing accurate information about the company and facility’s products, processes, plans, hazards, and risks. This encourages sharing of accurate process safety information to similar facilities within a company or industry group, as well as community groups that could be affected.

Process Knowledge Management

Developing, documenting, and maintaining process knowledge is the focus of this element and includes the following:

1. Written technical documents and specifications
2. Engineering drawings and calculations
3. Specifications for design, fabrication, and installation of process equipment
4. Other written documents such as material safety data sheets (MSDSs)
5. Process Hazard Analyses that are developed

Hazard Identification and Risk Analysis (HIRA)

Hazard Identification and Risk Analysis (HIRA) covers all activities involved in identifying hazards and evaluating risk at facilities. It involves the identification, evaluation, control, or risk transfer of potential hazards that may be associated with existing operations, new projects, acquisitions, and customer supplier activities.

This evaluation ensures that risks to employees, the public, and the environment are all evaluated, and that controls are implemented to minimize exposure.

Operating Procedures

The scope of this element is limited to those operating procedures that describe the tasks required to safely start up, operate, and shut down processes, including emergency shutdown. Operating procedures are normally used to control activities such as transitions between products, periodic cleaning of process equipment, preparing equipment for certain maintenance activities, and other activities routinely performed by operators. They are written instructions (including procedures that are stored electronically and printed on demand) that do the following:

1. List the steps for a given task.
2. Describe the manner in which the steps are to be performed.

Good procedures describe the process, hazards, tools, protective equipment, and controls in sufficient detail that operators understand the hazards, can verify that controls are in place, and can confirm that the process responds in an expected manner.

Specific procedures that address when an emergency shutdown should be executed as well as that deal with special situations, such as temporary operation with a specific equipment item out of service, are also valuable as are procedures for troubleshooting when the system does not respond as expected.

Safe Work Practices

This element covers practices for the control of hazards associated with maintenance and other non-routine work. Procedures are generally divided into three categories:

1. Operating procedures govern activities that usually involve producing a product.
2. Maintenance procedures generally involve testing, inspecting, calibrating, maintaining, or repairing equipment.
3. Safe work procedures, which are often supplemented with permits (i.e., a checklist that includes an authorization step), fill the gap between the other two sets of procedures. Safe work practices help control hazards and manage risk associated with non-routine work.

Asset Integrity and Reliability

Asset integrity is the element that helps ensure equipment is properly designed, installed in accordance with specifications, and remains fit for use until it is retired.

The asset integrity element is the systematic implementation of activities, such as inspections and tests necessary to ensure that important equipment will be suitable for its intended application throughout its life. Specifically, work activities related to this element focus on the following:

1. Preventing a catastrophic release of a hazardous material or a sudden release of energy
2. Ensuring high availability (or dependability) of critical safety or utility systems that prevent or mitigate the effects of these types of events

Contractor Management

The management of contractors poses unique challenges for a facility. This can result from the potential lack of familiarity that contractor personnel may have with plant hazards, operations, and procedures. Contractor management is a system of controls to ensure contracted services support both safe facility operations and the company's process safety and personal safety performance goals. This element addresses the selection, acquisition, use, and monitoring of such contracted services.

Training and Performance Assurance

This element addresses the training of workers to ensure their reliable performance of critical tasks. A documented training program is fundamental to achieving reliable worker performance. The jobs and tasks that workers are expected to perform must be identified, workers must be selected and trained, and their performance must be monitored on an ongoing basis. Performance assurance is the means by which workers demonstrate that they have understood the training and can apply it in practical situations. Performance assurance is an ongoing process to ensure that workers meet performance standards and to identify where additional training is required. The management system must be designed to accomplish those objectives consistently over the life of the process.

Management of Change

Management of change is necessary to ensure that alterations in a process do not inadvertently introduce new hazards or cause any existing hazards to present an increased risk. Management of change provides a system whereby proposed adjustments to facility design, operations, organization or activities prior to implementation are reviewed and authorized. Management of change also provides measures to allow affected personnel to be notified of any changes and that related documents and procedures and other key information are all updated as part of the process.

Operational Readiness

Throughout the life of a facility, there are times when processes and equipment are shut down. The shutdown period can be brief or it can be lengthy. In the worst case, shutdowns may be of an extended period, such as when equipment is idled (a condition known as “mothballing”). Common reasons for the shutting down of equipment include maintenance, modification, administrative decisions (e.g., due to lack of demand for a product) and weather (e.g., hurricane, flood).

This element ensures that shutdown processes are verified to be in a safe condition for restart. It is more broad in scope than the OSHA process safety management pre-startup safety review (PSSR) element in that it specifically addresses startup from all shutdown conditions, not only those resulting from new or changed processes.

Conduct of Operations

CCPS refers to this element as “operational discipline” or “formality of operations.”

Safety and environmental incidents are directly impacted by human errors within a facility. To ensure facilities operate and are maintained safely, reliable performance from all employees at all levels is needed.

Often seen as part of a policy, the conduct of operations element spells out observable standards of behavior for all employees in their work, including the execution of tasks associated with operations, maintenance safe work and emergency planning and response, as well as the overall management of the process and the risks. Typically, it spells out what activities are prohibited, permitted with no special controls and what procedures govern these activities. It also attempts to document the work practices that are widely understood but often unwritten within a particular facility. By formalizing them as such, these practices can be consistently taught and enforced.

Emergency Management

Activities relating to emergency management and response capabilities including pre-planning, training, drills and exercises, along with the applicable responses and resources required in emergency situations are covered by this element.

Most facilities have emergency plans in place. This element provides focus for these plans to ensure they cover the range of credible scenarios likely to occur at the particular facility and that they work when they are needed.

Incident Investigation

Incident investigation is the process for reporting, tracking, and investigating process safety incidents. Typically it involves a formal investigation process as well as the trending of the incident and the incident investigation data. The data is used to identify recurring incidents.

The process also manages the results of investigations along with the documentation that is generated during those investigations.

Measurements and Metrics

This element deals with the use of process safety metrics to measure the effectiveness of process safety systems present within a facility. Both leading and lagging indicators are used. The metrics can be used to address performance issues and/or efficiency issues within the process safety management structure.

Such performance monitoring allows for problems to be identified and corrective actions to be taken before a more serious incident occurs.

Auditing

Auditing is used to evaluate how the process safety management systems are performing. Through the analysis of the results, any corrective actions necessary are determined. This element is linked to several others elements within the risk based process safety program. Audits are key control mechanisms within the overall process safety management system and can provide benefits such as opportunities for improved operability, increased safety awareness and increased confidence in areas where compliance with regulatory bodies is needed.

Management Review and Continuous Improvement

Management review and continuous improvement is the evaluation of process safety management systems to ensure they are preforming as intended and producing the results that are needed as efficiently as possible. This element shares many characteristics of the auditing element, including the allocation of staff, time, and resources for the review process. It differs from auditing in that this element also includes the “due diligence” which exists between the daily work activities and the more structured formal audits, which are conducted periodically. Similarly this element also includes a system for implementing any resulting improvement plans that are generated and also monitoring their effectiveness.