Safety Procedures and Designs

- Process accidents are prevented by managing the development and maintenance of important process activities.
- This chapter covers the details of this management process by focusing on the following topics:
    - Process safety hierarchy
    - Managing safety
    - Best practices
    - Procedures—operating
    - Procedures—permits
    - Procedures—safety reviews and accident investigations
    - Designs for process safety
    - Miscellaneous designs for fires and explosions
    - Designs for runaway reactions
    - Designs for handling dusts

- The motivation for including many of these topics is based on four well-known paraphrased quotations:

  (1) The causes of accidents are visible the day before the accident;

  (2) we are not inventing new ways to have accidents;

  (3) learn from history or you're doomed to repeat it

  (4) sometimes doing your best is not enough— sometimes you need to do what is required.

Process Safety Hierarchy

Process Safety Strategies

- There are four categories of process safety strategies, in order of preference:

  (1) inherent,

  (2) passive,

  (3) active, and

  (4) procedural

- **Inherent:** Identify and implement ways to completely eliminate or significantly reduce hazards, rather than to develop add-on protective systems and procedures. Inherently

- **Passive:** Add safety features that do not require action by any device. Passive devices perform their intended functions without personnel or control actions. Passive systems include dikes, passive flame arrestors, and the use of welded fittings versus flanges and threaded connections.
- **Active:** Add safety shutdown systems to prevent accidents. Active systems include process control systems, safety interlocks, automatic shutdown systems, and automated mitigation systems.
- **Procedural:** Include standard operating procedures, safety rules, operator training, emergency response procedures, and management techniques in general.

Inherent and passive strategies are the most robust and reliable, but elements of all strategies are required to minimize safety problems.

Layers of Protection

- These layers are necessary because it is unlikely that inherently safer design features alone will eliminate all hazards. Each layer reduces the process risk.
- Active and procedural layers of protection require constant maintenance and management to ensure that they continue to function as designed.
- If they are not managed correctly, the protection systems will degrade and increase the hazards to an unacceptable level.
- Inherently safer designs make these layers of protection more reliable and robust.

Managing Safety

In the area of safety, this simple process is adapted to include

- **Documentation:** Describe what needs to be done to eliminate hazards and accidents.
- **Communication:** Motivate everyone influenced by this document to do what needs to be done.
- **Delegation:** Delegate portions (manageable parts) of the responsibilities to those involved.
- **Follow-up:** Check to be sure that the documentation (procedures, etc.) is used as intended. Also use this follow-up process to make improvements.

Best Practices

- Engineers have the responsibility to use best practices when designing and operating Plants.
- The AIChE Code of Ethics states that engineers must perform professional services only in areas of their competence.
- Many accidents investigated by CSB were due to the failure to use the codes, standards, and other Recognized and Generally Accepted Good Engineering Practices (RAGAGEP).

Sources of RAGAGEP include

- Government laws
- American Petroleum Institute (API) standards
- AIChE's Center for Chemical Process Safety (CCPS) guidelines
- National Fire Protection Association (NFPA) fire codes and standards
- Methods and rules in engineering texts
- Industrial experience acquired by sharing information within industry

some of the most widely used best practices documents include those by CCPS, NFPA, API, and OSHA.

Procedures—Operating

- Operating procedures are designed and managed to help operators run a plant or facility with no problems or mishaps.
- They should include steps for each operating phase and operating limits for the startup, shutdown, normal, temporary, and emergency procedures.
- Additionally, they should
  - (1) contain engineering and administrative controls for preventing exposures,
  - (2) include a description of the controls that are needed for safe operation,
  - (3) highlight the permits that are used to control the environment.

Procedures—Permits

- Permits are used to control non-routine activities that are conducted in potentially hazardous environments.
- The permit includes a description of the hazards and actions taken to prevent accidents.
- The formal permit communicates relevant information between the people doing the work and the operating personnel who are affected by the work.
- The required permit actions include those by the workers and the operators;
- they include
  - Actions before the work is permitted and actions after the work is completed to transition from the permitted environment to the normal operating mode.

- The following examples give the key features of a few permits

Hot Work Permit

- This permit prevents the ignition of flammable or combustible gases or liquids in a work environment.
- Hot work operations include welding, grinding, torch cutting or soldering, and any other ignition sources. These permits are valid for only one shift at a time.
- The procedure includes the following:

  1. Check for flammable materials in areas and trenches with a flammable gas detection meter.

  If there are flammable vapors in the area, then a permit is not allowed.

2. Remove all containers of flammable and combustible materials within a 35-foot radius of the hot work. If they can't be removed, then cover them with a flame Retardant tarp and post the area with a fire watch.

3. Place a fire extinguisher in the area, and check to be sure that smoke detection, sprinkler, and alarm systems are working.

4. Inform operations and everyone in the area and then post the signed permit.

Also, maintain a file of past permits.

Lock-Tag-Try Permit

- This permit prevents injuries or damage due to the accidental release of stored energy from equipment.

- The stored energy includes electrical, gravitational, mechanical, and thermal.
- This permit is intended to prevent equipment from unexpectedly being set into motion and endangering workers.
- Employee going into a danger zone (rotating equipment or in a vessel with an agitator),
- Repairing electrical circuits, maintaining machinery with moving parts, cleaning jammed mechanisms, and removing guards or safety devices.

- The lock-tag-try procedure starts with a de-energize process:
  - De-energize the equipment by unplugging electrical connections; releasing pressured lines such as hydraulic, air, steam, gas and water; and releasing spring-loaded devices.
  - Lock the equipment or electrical device to prevent reactivation. A gang lock device is used to allow the device to be locked out by several maintenance trades and operations personnel.
  - Tag the equipment or device to warn against re-energizing the equipment. Tags alone can be used only when the equipment cannot be physically locked, for example, some valves.
  - Try to re-energize the equipment to verify that the locking process works.
  - Prior to going back to the normal operation, the operations supervisor is the last one toremove the lock, after being certain that the device or equipment is safe to re-energize

Vessel Entry Permit

This permit is sometimes called the confined space permit. It is used to prevent someone from being injured in a confined space. The confined space could be a vessel, a diked area, or even reaching into a large pipe opening.

The permit includes the following steps:

1. Have an area supervisor take complete control of the vessel entry according to the permit details.
2. Isolate the equipment by disconnecting all process lines going into the vessel, which may include activating double block and bleed systems.
3. Clean the equipment.
4. Manage all other permits on this system, including lock-tag-try and hot work permits, to prevent inadvertent activation.
5. Have a second attendant in the area to help with emergencies.
6. Place emergency equipment in the area, such as a fire extinguisher.

7. Place safety cuffs around the entering person's wrists with a chain and pulley to enable removal of the person under emergency situations.

8. Continuously monitor the oxygen concentration to be sure that it is at least 19.5%.

9. Add ventilation in the vessel or confined space to be sure the concentration of oxygen is maintained.

10. Have a ground fault interrupting light to assist the person's visibility in the vessel.

11. Have a two-way radio at the vessel to summon help if required.

12. Use a ladder to enter the vessel, unless step-down distance is small compared to the height of the person entering.

13. Have the manager in charge sign the permit and post it in the area.

Procedures—Safety Reviews and Accident Investigations Safety Reviews

Major focus of a review is to improve procedures and designs. In this regard, some of the features of safety reviews include the following:

1. Develop and review detailed process descriptions. This description should include

(a) a process flow diagram (PFD)

(b) a piping and instrumentation diagram(P&ID)

(c) a layout to show the relationship of the equipment.

2. Accumulate and review the chemical, physical, and reactive properties of all chemicals in the plant.

- The list of chemicals should include all combinations of the chemicals being used in the process, and the the chemicals plus possible contaminants.

3. Develop and review operating procedures, including startup, shutdown, normal, and emergency procedures.

The operating procedures should highlight the limitations of the process (e.g., temperature and pressure) and give the consequences when the limitations are exceeded.

4. Accumulate and review accident investigations of previous and relevant incidents that are shared throughout the company and between companies.

5. Develop recommendations to improve the design and operating procedures to eliminate hazards and prevent accidents.

6. Develop and review the management system to ensure that all of the safety review recommendations are implemented and documented before the startup.

A typical accident investigation report format is shown

Accident title:
Major damage:
Date:
Location:

Events

1. Major accident scenario:
2. Pre-accident conditions:
3. Events that precipitated the accident:

Typical Accident Report

Causes of accident

1. Design problems
2. Control problems
3. Problems in the operating procedures
4. Management problems, including maintenance and bad decisions

Recommendations for prevention/mitigation

1. 1st layer: Immediate technical recommendation: specific changes to the design, operating procedures, maintenance, etc.
2. 2nd layer: Recommendations for avoiding the hazard: clearly specifying process limitations and the consequences of deviations.
3. 3rd layer: Recommendation for improving the management systems; add annual audits to be sure the new designs and operating procedures are used as specified, and add periodic training.

Designs for Process Safety

There are some key safety features for Designs

Inherently Safer Designs

- It is possible that a modification in one area may increase or decrease a hazard in another area.
- An engineer, therefore, should evaluate alternative inherently safer designs, in order to choose the best inherently safer design.
- In these cases a decision tool is used to evaluate the options to identify the best designs.
- The tools include voting methods, weighted scoring methods, cost-benefit analysis, and decision analysis.

A simple summary description of inherent safety includes four alternatives:

1. Moderate: Use milder conditions.
2. Substitute: Replace hazardous with non hazardous chemicals.
3. Minimize: Use smaller vessels (reactors or storage) and quantities.
4. Simplify: Design systems to be easy to understand, including the mechanical designs and computer screens.

Inherent Safety Techniques

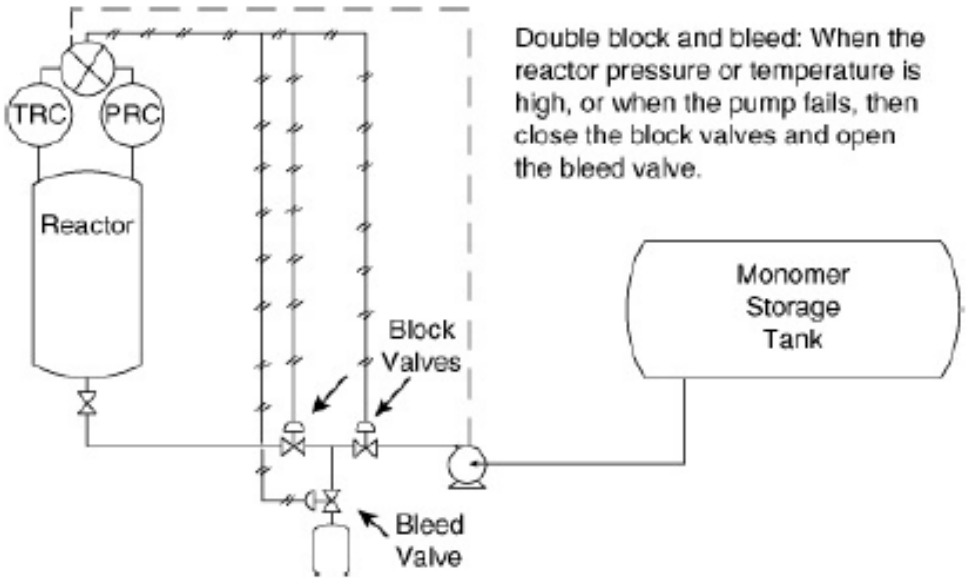
Type	Typical techniques
Minimize (intensification)	Change from large batch reactor to a smaller continuous reactor Reduce storage inventory of raw materials Improve control to reduce inventory of hazardous intermediate chemicals Reduce process hold-up
Substitute (substitution)	Use mechanical pump seals vs. packing Use welded pipe vs. flanged Use solvents that are less toxic Use mechanical gauges vs. mercury Use chemicals with higher flash points, boiling points, and other less hazardous properties Use water as a heat transfer fluid instead of hot oil
Moderate (attenuation and limitation of effects)	Use vacuum to reduce boiling point Reduce process temperatures and pressures Refrigerate storage vessels Dissolve hazardous material in safe solvent Operate at conditions where reactor runaway is not possible

	Place control rooms away from operations
	Separate pump rooms from other rooms
	Acoustically insulate noisy lines and equipment
	Barricade control rooms and tanks
Simplify (simplification and error tolerance)	Keep piping systems neat and visually easy to follow
	Design control panels that are easy to comprehend
	Design plants for easy and safe maintenance
	Pick equipment that requires less maintenance
	Pick equipment with low failure rates
	Add fire- and explosion-resistant barricades
	Separate systems and controls into blocks that are easy to comprehend and understand
	Label pipes for easy "walking the line"
	Label vessels and controls to enhance understanding

Controls—Double Block and Bleed

- Double block and bleed systems are installed,

  for example, in monomer lines between the reactor and the monomer feed tanks
- This prevents the reactor contents, including catalysts, from inadvertently backing up into the monomer tank.
- When the pump fails, the double block and bleed is activated, and it is virtually impossible to transfer reactor contents to the monomer tank.



Controls—Safeguards or Redundancy

- Safeguards or redundant controls are a special set of controls that are added to a system to reduce the possibility of an accident.
- For example, a reactor that controls a rapid and exothermic reaction should have a group of safeguards to prevent the hazardous runaway.
- Redundancy increases the reliability of a control system; the quantitative effects of redundancy are computed using fault tree analysis

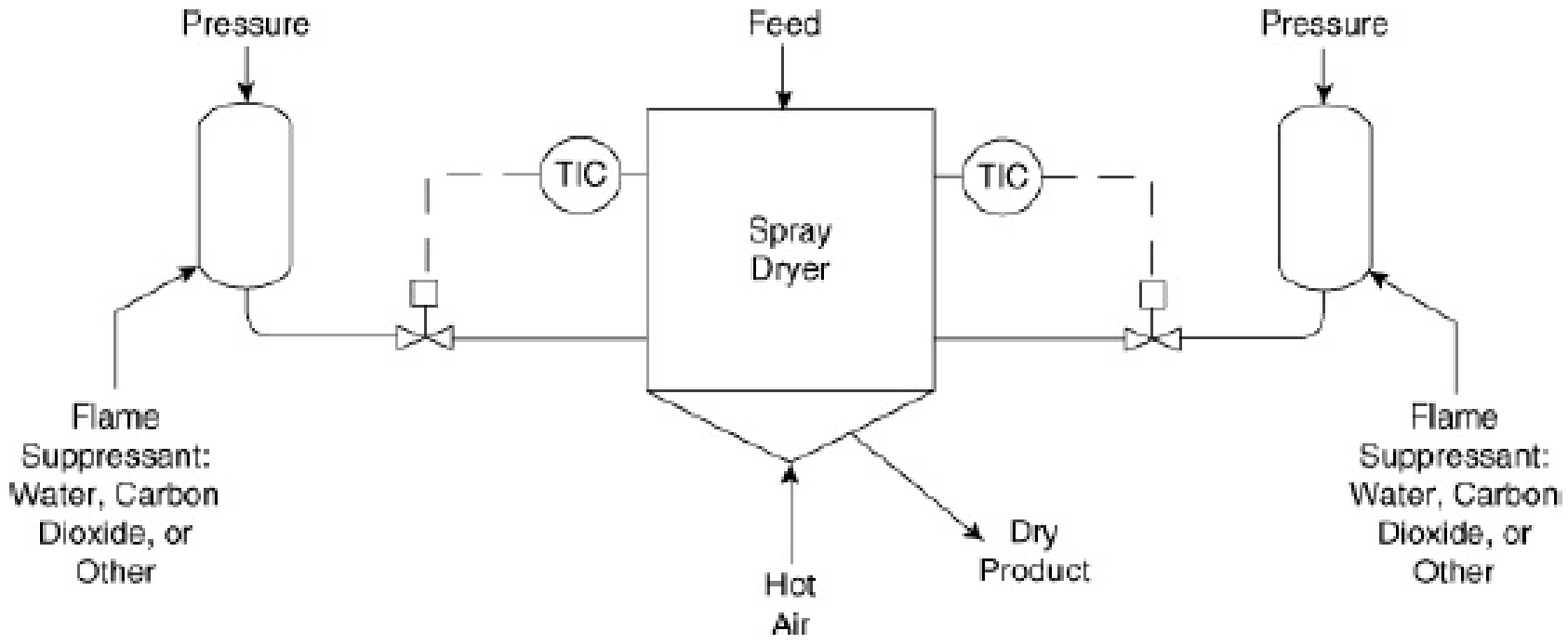
Controls—Block Valves

- Block valves are installed throughout plants to shut a system down during unusual circumstances. Block valves can be manually operated or operated by a control system or field analyzer.
- Block valves typically are installed in lines at all vessels containing hazardous materials, and activated when an adjoining line or hose develops a leak.
- Installed in sewer lines to prevent major leaks from contaminating a treatment facility; and sometimes installed in plants so that materials can be transferred from a hazardous environment to a safe one.
- Example: when a fire is around a vessel, a normally closed block valve would be opened to transfer the material to a safe location.

Controls—Explosion Suppression

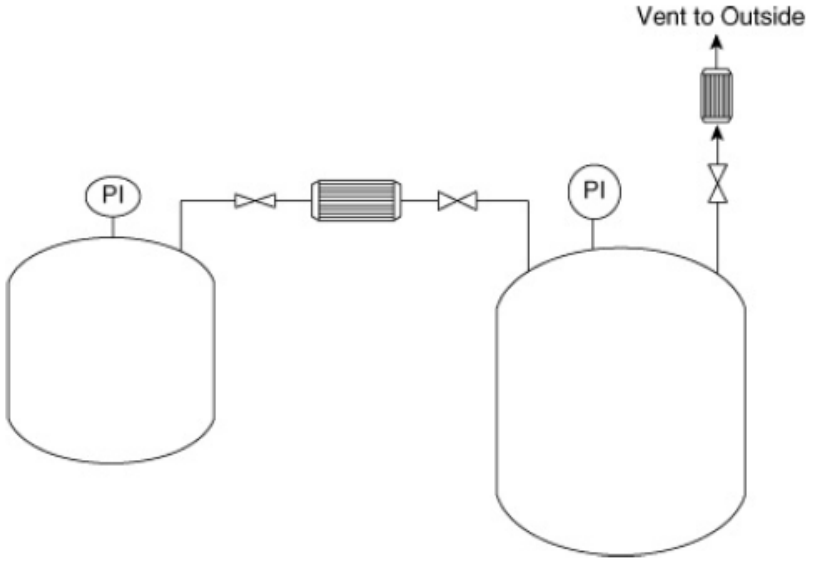
- A explosion suppression system detects a flame or pressure at the incipient phase of an explosion or fire.
- This detection system sets off quick-acting valves to inject a flame-quenching substance into the burning region.
- This type of system can be installed in pipelines, to prevent a fire from going from one vessel to another.
- it can also be used outside equipment to detect and quench fires or explosions.

The one illustrated in this figure would prevent the explosion of the spray dryer.



Flame Arrestors

- Flame arrestors are placed inline or at the end of a line.
- In both cases these devices quench a flame, preventing it from propagating down a pipe or duct containing a flammable.

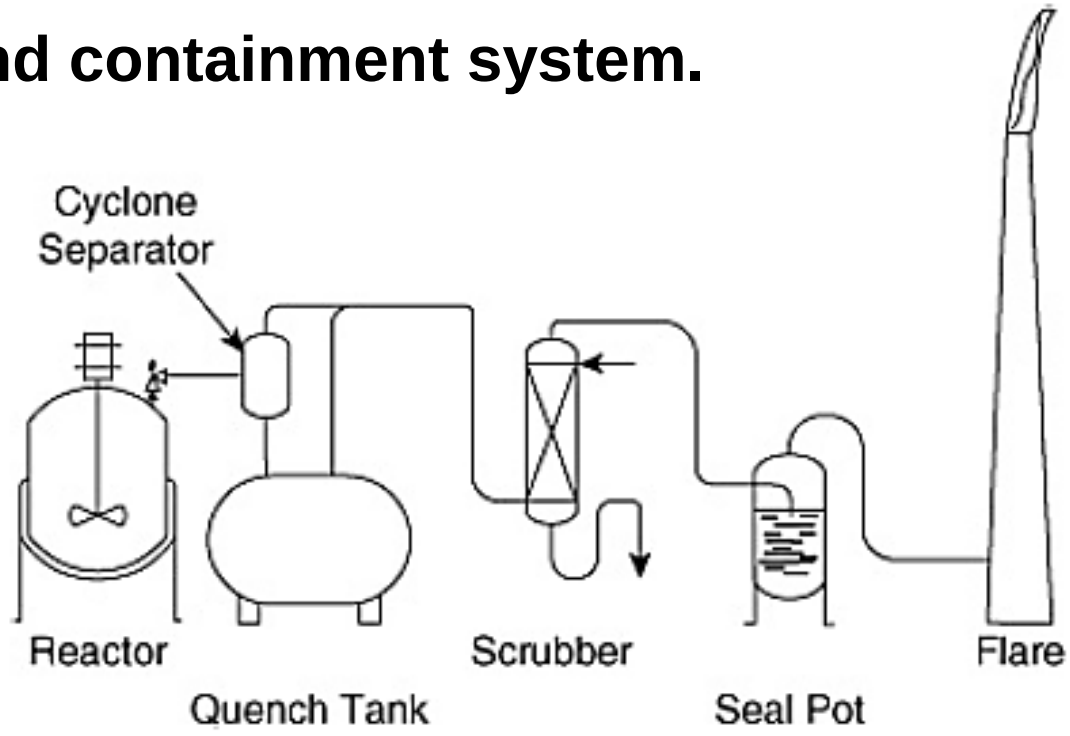


- As shown in this figure, the end-of-line flame arrestor prevents a burning gas from propagating back to the vessel, if the vent gas is ignited by lightning.

Containment

- With a chemical that is especially hazardous, the exits of a relief system should go to a containment system.
- When containment is used, however, it is very important that a detailed management system be used to ensure it is always maintained and operational.

Relief and containment system.



Materials of Construction

- Material failures can occur without warning, resulting in large accidents. The way to reduce the risk of corrosion failures is to fully understand the internal and external environments, and to specify the materials of construction to withstand this environment.
- There was an accident in an oil refinery due to an error in the welding process.
- The welder used a weld material that was less noble then the tower’s material of construction.
- Therefore, corrosion transferred the less noble weld material to the tower.
- The weld seam around the entire tower failed, and the tower fell with major adverse consequences

Process Vessels

- Process vessels are designed to withstand the temperatures, pressures, and corrosion environments of the process.
- Normally, the thickness of the vessel is chosen to withstand the pressure, and the thickness is increased for a corrosion allowance.
- The corrosion allowance is based on laboratory determinations of the corrosion rate and the desired life of the vessel.
- Process vessels are designed to withstand the temperatures, pressures, and corrosion environments of the process.
- Normally, the thickness of the vessel is chosen to withstand the pressure, and the thickness is increased for a corrosion allowance.
- The corrosion allowance is based on laboratory determinations of the corrosion rate and the desired life of the vessel.

- For cylindrical vessels with the pressure p not exceeding 0.385 times the mechanical strength of the material $S_{M.}$

$$p = \frac{S_M t_v}{r + 0.6 t_v},$$

p is the internal gauge pressure,

S_M is the strength of the material,

t_v is the wall thickness of the vessel, and

r is the inside radius of the vessel.

- For cylindrical vessels and pressures exceeding 0.385*S*M, the following equation applies

$$p = \frac{S_M\left(\frac{t_v}{r} + 1\right)^2 - S_M}{\left(\frac{t_v}{r} + 1\right)^2 + 1}.$$

- For spherical vessels with pressures not exceeding 0.665*S*M the equation is

$$p = \frac{2 t_v S_M}{r + 0.2 t_v}.$$

- For spherical vessels and pressures exceeding 0.665 S_M the equation is

$$p = \frac{2S_M\left(\frac{t_v}{r} + 1\right)^2 - 2S_M}{\left(\frac{t_v}{r} + 1\right)^2 + 2}.$$

Material	Tensile strength (psi)	Yield point (psi)
Borosilicate glass	10,000	
Carbon	660	
Duriron	60,000	30,000
Hastelloy C	72,000	48,000
Nickel	65,000	48,000
Stainless 304	80,000	35,000
Stainless 316	85,000	40,000
Stainless 420	105,000	55,000

Deflagrations

- Breaks in pipes or vessels resulting from deflagrations or simple over pressurizations are usually tears with lengths no longer than a few pipe diameters.
- The pressure increases during deflagrations are approximately

$$\frac{p_2}{p_1} \approx 8 \text{ for hydrocarbon-air mixtures,}$$

$$\frac{p_2}{p_1} \approx 16 \text{ for hydrocarbon-oxygen mixtures.}$$

Detonations

- Detonations have a rapidly moving flame and/or pressure front.
- Detonation failures usually occur in pipelines or vessels with large length-to-diameter ratios.

Detonations

- Detonations have a rapidly moving flame and/or pressure front.
- Detonation failures usually occur in pipelines or vessels with large length-to-diameter ratios.
- In a single vessel detonations increase pressures significantly

$$\frac{p_2}{p_1} \approx 20.$$

- When a pipe network is involved, the downstream p_1 increases because of pressure piling; therefore p_2 may increase by as much as another factor of 20.
- They usually occur at pipe elbows or other pipe constrictions, such as valves. Blast pressures can shatter an elbow into many small fragments.

In pipe systems explosions can initiate as deflagrations and the flame front may accelerate to detonation speeds.

Miscellaneous Designs for Fires and Explosions

Designs for Runaway Reactions

The essential requirements to prevent runaway reactions include

- Understanding the concepts and hazards of runaway reactions
- Characterizing all possible runaway reactions in the specific system being designed
- Using this knowledge to design the equipment and controls to avoid runaways.
- The equipment features may include a semi-batch reactor versus a batch, and the
- Controls may include redundancy and double block and bleeds in the monomer feed lines

Some of the other design features that are used to prevent runaways include the following:

1. Design to consume the reactants rapidly to avoid the accumulation of reactants.
2. Design the system to remove the heat and gaseous products generated by the reactions.
3. Use semi-batch reactors instead of batch and add the reactants at rates to control monomer concentrations, that is, lower concentrations that prevent excessive pressures and releases with the accidental loss of cooling.
4. Add safeguards to prevent runaways due to equipment and control failures. The equipment failures may be pumps, agitators, and so on and the control failures may be temperature and pressure controls.

- In cases like these, redundant control loops would catch the failure and activate a safe shutdown of the reactor system.
- heat removal is more difficult with larger reactors, avoiding adding materials at temperatures above the reactor contents, and knowing that reliefs for runaway reactions need to be designed for two-phase flow.
-

Designs for Handling Dusts

- The safe handling of solids is important because many chemicals are produced as solids to eliminate the transportation of hazardous solvent diluents.
- Dusts, have flammability regions similar to gases, and they can burn and explode as deflagrations and detonations.
- The added problem with dusts, however, is that primary explosions can, and usually do, initiate secondary explosions as the explosion forces and turbulence disperse dusts that may have accumulated on floors, inducts, or above false ceilings.
- Flammable dusts have the five-sided fire pentagon that includes fuel, an ignition source, oxygen, low moisture, and suspension in air.

Designs for Preventing Dust Explosions

- Some of the key design features that are used to prevent dust explosions include the following:

1. When transferring dusts to flammable liquids, use containment and inerting.

2. Eliminate ignition sources due to tramp metal, mechanical failure, overheating, electrical sparks, high dust concentrations, and static electricity.

- The tramp metal problem: is solved by adding magnetic traps that collect metal parts;
- the mechanical failure problems: are solved by adding detectors to detect failures and initiate a safe shutown;

- overheating problems: are solved by monitoring the temperature of bearings and belts (e.g., slipping);
- electrical sparks: are eliminated by using all explosion-proof electrical fittings
- High dust concentrations: in equipment and in vents from equipment are reduced by using pneumatic dust collection systems (sometimes called bag houses)
- High dust concentrations outside of equipment due to leaks from flanges or equivalent are prevented by adding gaskets and tightening the gasket flanges;
- static electricity problems are solved using the teachings of including grounding and bonding.

3. Mitigate dust explosions using vent panels and explosion suppression.

Management Practices for Preventing Dust Explosions

There are two especially important management practices that should be used to prevent dust explosions:

(1) Schedule periodic cleaning to remove accumulated dusts from floors, ducts, and even above false ceilings

(2) Control welding and cutting operations using the hot work permits discussed previously.

Additional recommended practices include scheduling the periodic cleaning of the magnetic tramp metal traps and mechanical integrity checks to be sure all controls and alarms are working as specified.