SKF 4163 : Safety in Process Plant Design

Inherent Safety

MOHD FADIL ABDUL WAHAB
Faculty of Petroleum and Renewable Energy Engineering

NORZITA NGADI
ARSHAD AHMAD
MOHD WIJAYANUDDIN MOHD ALI
Faculty of Chemical Engineering

Let's first talk about Human Factor in Safety

Some Facts!

It should be understood by all operation

96% of all accidents are related to unsafe behaviours (e.g. shortcut)

4% of accidents are caused by unsafe conditions (eg. wet floor)

Causal Factors for Accidents

Human Performance:

- Training/qualification
- Verbal communication
- Written procedures & documents
- Environmental condition
- Work schedule
- Work practices
- Work organization/planning
- Supervisory methods
- Change management
- Resource management
- Managerial method
- Man-machine interface

Causal Factors for Accidents

Equipment:

- Design configuration & analysis
- Equipment condition
- Environmental condition
- Equipment specification, manufacture & construction
- Maintenance/testing
- Plant/system operation

Type of Unsafe Acts (Errors)

- Direct
  - Errors carry out by users/operators of equipment / the one executing the action
  - Intentional vs Unintentional

- Indirect
  - Fallible decisions made by committee etc
    - Management, engineering, design etc

Note: Indirect Unsafe Act is related to Root Cause of an accident.

Intentional Direct Unsafe Act

- Intentional Unsafe Act is called Violation
- Violation involve deliberate deviation from procedure
  - Short cut
  - Well-intentioned experiment
  - Sabotage
- Violation is a behavioral problem
  - Must be addressed by changing attitudes at work place.
  - Need to improve morale of workers, provide training etc…

Unintentional Individual's Direct Act

Related to the ability/inability to make correct judgment.

This is called errors. There are 2 types of errors.

- Mistake – error in deciding the type of action required
  - Lack of knowledge (mismatch), wrong decision
- Slips - an error that occurs as a result of forgetfulness, habit, fatigue or similar psychological causes.
  - Interruptions, phone calls etc

Indirect Unsafe Acts

- Fallible decision made by management, engineering etc…(remember root cause of accident)

- Organizational failure
  - Maintenance, decision, work environment, operational procedure, communication, monitoring, improper safety procedures, lack of training etc…

Individuals should not be blamed* for accidents !

- No responsible person would deliberately do something to injure themselves or friends!
- Individuals are involved directly or indirectly in any accidents

* But someone will be held responsible………

Accidents Cause Many

- Lives, injuries, damages to plant and equipment
- Loss production
- Increased costs
  - Insurance, medical, rehabilitation, training and retraining
- Lowering of workplace morale
- Substantial loss of market share
- Loss of Profitability

Closure

- Not all accidents are preventable but level of risk (frequency and severity) of accidents can be reduced or minimized by
  - Careful forethoughts
  - Planning
  - Strict adherence to safe work practices

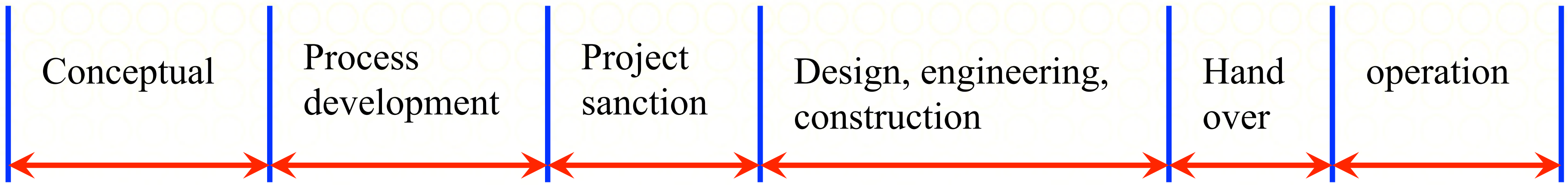
Inherent Safety Concept

Inherent Safety Concept

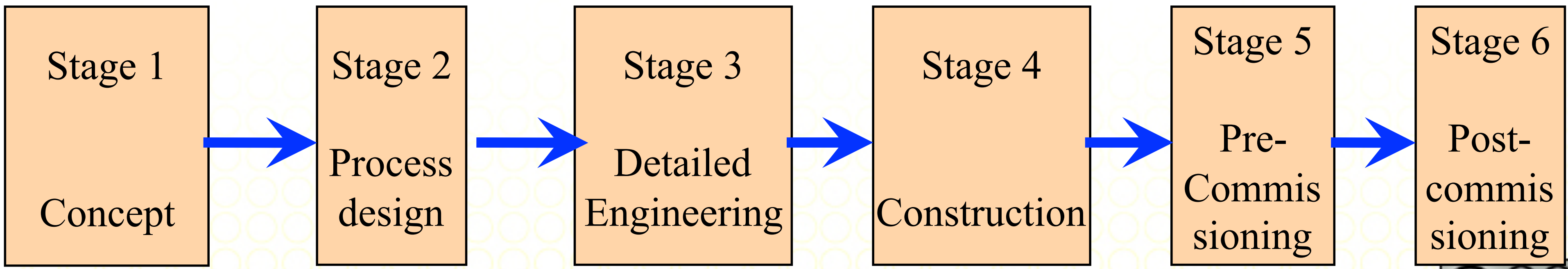
- To reduce the risk at early stage of design

PROJECT PHASE

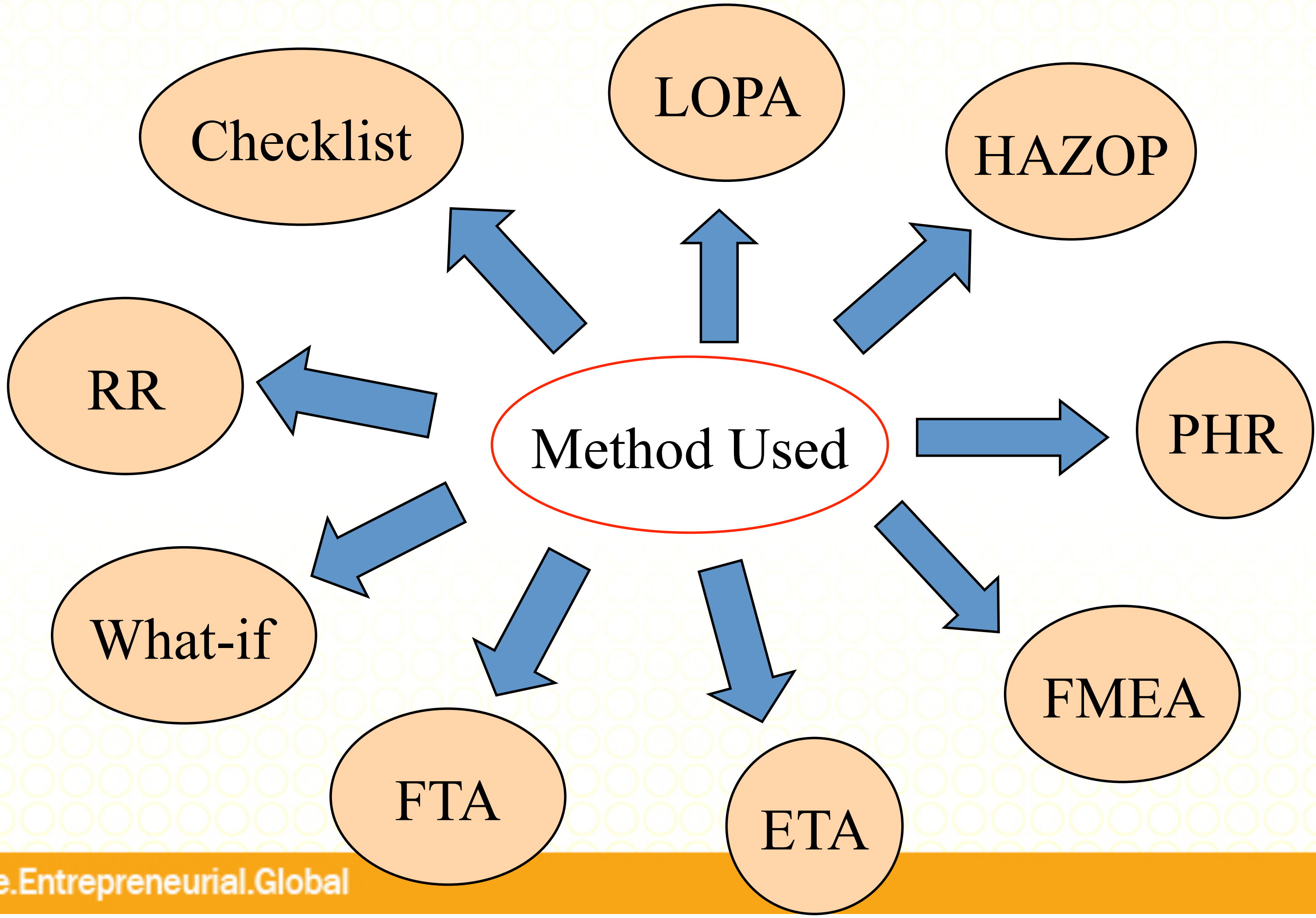
Safety issues must be embedded within all project life-cycle



<u>Relationship of six-stage process study system to project life-cycle</u>



Many hazard identification technique can be used at appropriate cycle



Inherent Safety

Inherent safety is to develop a process (chemistry and physics) which is by nature a safer process.

Usually perform at the earliest stage of process development/design.

Also cost effective (e.g. design at lower T and P operation results in lower capital and operating cost)

More tolerant to operator errors

The application of inherent safety is based in the following keywords (ISAS):

- **Intensification**
- **Substitution**
- **Attenuation**
- **Simplification**

Intensification (minimization)

Examples,

- ✓Use smaller continuous reactors instead of large batch reactor.
- ✓In situ production and consumption of hazardous chemical
- ✓Reduce storage inventory of raw materials
- ✓Reduce inventory of hazardous intermediate chemicals
- ✓Reduce process hold-up (delay)

Substitution

Examples,

- ✓ Avoid using hazardous material, but instead, use a safer one.
- ✓ Use welded pipe instead of flanged/threaded pipe
- ✓ Use solvents that are less toxic
- ✓ Use chemical with higher flash point, boiling point and other less hazardous properties
- ✓ Use water as heat transfer fluid instead of hot oil

Attenuation (moderation and limitation of effects)

Examples,

- ✓ Use vacuum to reduce boiling point
- ✓ Use less severe temperature and process conditions
- ✓ Liquefied gases can be stored as refrigerated instead of under pressure.
- ✓ Dissolve hazardous material in safe solvent
- ✓ Operate at conditions where reactor runaway is not possible
- ✓ Handling larger particle size solid to minimize dust
- ✓ Use of hazardous materials under the least hazardous conditions.
- ✓ An explosive powders are better in slurries forms rather than dry to avoid dust explosion.

Simplify (simplification and error tolerance)

Examples,

- ✓ Keep piping systems neat and visually easy to follow (label, colour coding)
- ✓ Design control panel that are easy to comprehend
- ✓ Design plant for easy and safe maintenance
- ✓ Use equipment that require less maintenance
- ✓ Label vessels

Example: Choice of process

- Choose process which is less hazardous - this includes intermediate products, reagent, compatibility of materials, catalysts and also solvents used.
- Production of ketone-aldehyde (KA) at Flixborough
  - It is an intermediate for nylon production.
  - Before accident, KA produced by **air oxidation of cyclohexane.**
  - After accident and plant rebuilt, alternative route (substitution) of process by **hydrogenation of phenol** was chosen. This is vapor phase process and less hazardous than oxidation of cyclohexane.

Example: Reactor Design

- Reactors are usually large because reactions are slow and conversion is often low.
- To improve mixing try reduce reaction volume (intensification)
- Speed up the reaction by using a proper catalyst.
- Selection a proper type of reactor.
- For example, with oxidation of liquid cyclohexane the reaction of KA mixture was carried out in reactor fitted with external cooler, pump as well as stirrer. Instead, the gas phase hydrogenation of phenol uses internally cooled plug flow reactor.

Example: Distillation Column Design

- Distillation column usually held up large inventory of boiling liquid.
- So, try to reduce inventory through :
  - minimize size of column, use many small column instead of one big one (intensification)
  - use special design which can reduce inventories and also residence time.
- For example, ICI Higee Distillation column - distillation takes place in rotating packed drum.

Example: Storage Installation

- Avoid storage by plant relocation - i.e. relocate producing and consuming plant near each other so that to avoid storing and transporting hazardous materials.

- Storage in safer form - for example,

  Some dyestuffs can be supplied as pastes instead of powders to avoid dust explosion.

  Liquid NH_3 stored through refrigeration at atmospheric pressure instead of stored as compressed liquid at ambient temperature.

So, in general;

- Good concept, but in some cases are not feasible due to many reasons. (cost, time , technology, location)

- Trade-offs are often implemented

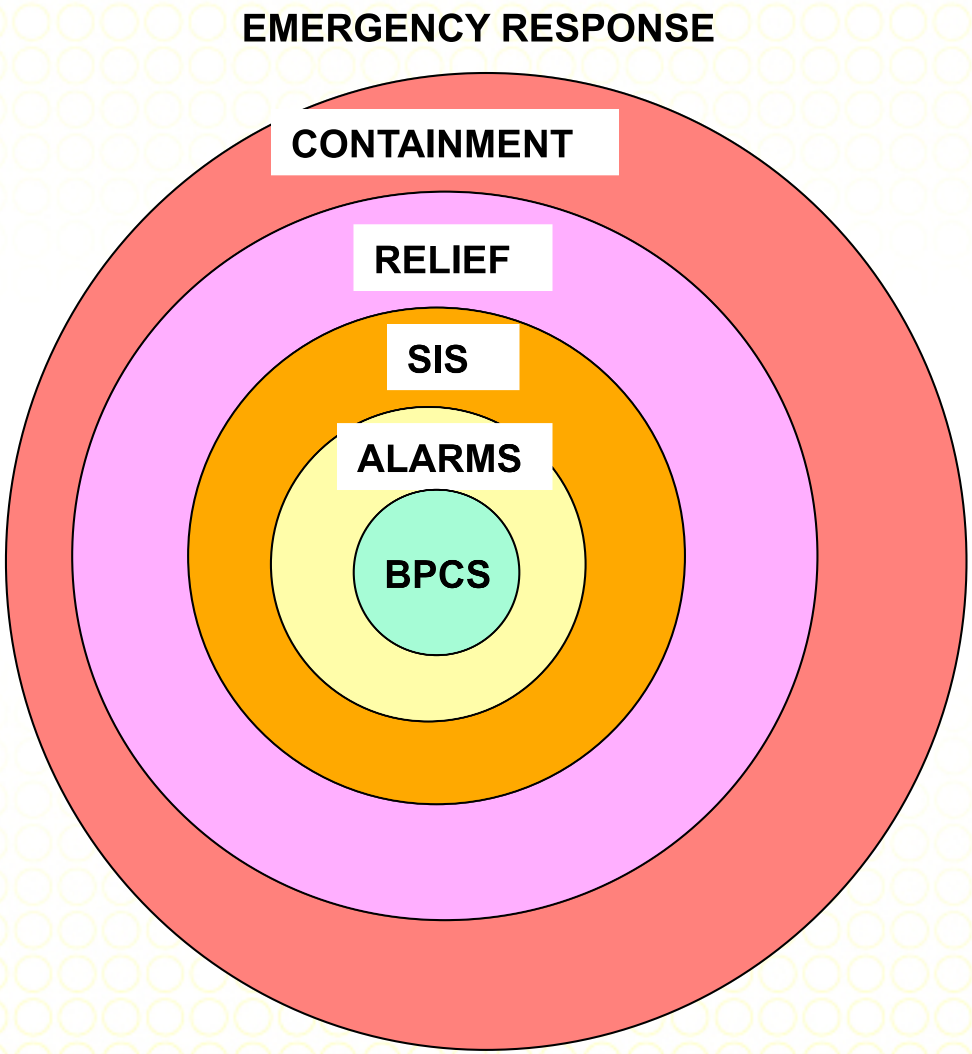
- Layers of protection are implemented to provide additional safety.

Layers of Protection in Process Plant

Key Concept in Process Safety:

Redundancy!!!!!

6 Layers of Protection for High Reliability



Protection Layers	Type of Device
Inherent safety in process design	Passive
1. Basic process control system (BPCS)	Active
2. Critical Alarms and Human intervention	Active/Human action
3. Safety intrumented functions (SIFs), e.g. Interlock	Active
4. Physical protection such as relief devices	Active
5. Post-release physical protection such as dikes	Passive
6a. Plant Emergency Response	Human action
6b. Community Emergency Response	Human action

Four independent layers of protections ILP, (automation)

Seriousness of event ↑

4. Relief system	Divert material safely
3. SIS	Stop the operation of part of the process
2. Alarm System	Bring unusual situation to attention of a person in the plant
1.BPCS	Maintaining process within acceptable operating region

PROCESS

Objectives of Process Control

1. Safety
2. Environmental Protection
3. Equipment Protection
4. Smooth Operation &
   Production Rate
5. Product Quality
6. Profit
7. Monitoring & Diagnosis

We are emphasizing these topics

1. BPCS

The Basic Process Control System (BPCS) is responsible for normal operation of the plant.

Normally use in the first layer of protection against unsafe conditions.

If the BPCS fails to maintain control, alarms will notify operations that human intervention is needed to reestablish control within the specified limits.

If the operator is unsuccessful then other layers of protection, e.g. pressure safety valves and SIS need to be in placed to bring the process to a safe state and mitigate any hazards.

2. Alarm System

- Alarm has an annunciator (visual indication)

  - No action is automated!

  - Require analysis by a person

  - A plant operator must decide.
- Digital computer stores a record of recent alarms
- Alarms should catch sensor failures

- Common error is to design *too many alarms*

  - Easy to include; simple (perhaps, incorrect) fix to prevent repeat of safety incident

  - One plant had 17 alarms but operator acted on only 8%

- Establish and observe clear priority ranking

- HIGH	= Hazard to people or equip., action required
- MEDIUM	= Loss of RM ($), close monitoring required
- LOW	= investigate when time available

3. Safety Interlock System

Also known as,

Safety Intrumented Functions,

Safety Intrumented Systems, or

Emergency shutdown system (ESS)

An additional safety layer designed to achieve specific Safety Integrity Levels (SILs) according to standard in IEC 61508 and IEC 61511

IEC:International Electrotechnical Commission

- **Automatic action usually stops part of plant operation to achieve safe conditions**

  - Can divert flow to containment or disposal
  - Can stop potentially hazardous process, e.g., combustion

- **SIS prevents "unusual" situations**

  - We must be able to start up and shut down

- SIS should respond properly to instrumentation failures
- Extreme corrective action is required and automated

  - More aggressive than process control (BPCS)
- Alarm to operator when a SIS takes action

4. Safety Relief System

- Entirely self-contained, no external power required
- The action is automatic - does not require a person
- Usually, goal is to achieve reasonable pressure

  - Prevent high (over-) pressure
  - Prevent low (under-) pressure

- The capacity should be for the "worst case" scenario

RELIEF SYSTEMS IN PROCESS PLANTS

Increase in pressure can lead to rupture of vessel or pipe and release of toxic or flammable material

- also we must protect against unexpected vacuum!

Naturally, best to prevent the pressure increase

- large disturbances, equipment failure, human error, power failure,

Relief systems provide an exit path for fluid

Benefits: safety, environmental protection, equipment protection, reduced insurance, compliance with governmental code

Location of Relief System

Identify potential for damage due to high (or low) pressure (HAZOP Study)

In general, closed volume (vessel) with ANY potential for pressure increase

- may have exit path such as hand valve, control valve (even fail open)

Remember, this is the last resort, when all other safety systems have not been adequate and a fast response is required!

Standard Relief Method: Pressure Safety Valves

BASIC PRINCIPLE: No external power required -
self actuating - pressure of process provides the needed force!

VALVES - close when pressure returns to acceptable value,
Type of relief valves:

- Relief Valve - liquid systems
- Safety Valve - gas and vapor systems including steam
- Safety Relief Valve - liquid and/or vapor systems

Pressure of protected system can exceed the set pressure.

Standard Relief Method: Rupture Disk

BASIC PRINCIPLE: No external power required - **self acting**

RUPTURE DISKS (OR BURST DIAPHRAGMS) - must be replaced after rupture (use only once)

.

Pressure Safety Valves

Two types of designs determine influence of pressure immediately after the valve

- **Conventional Valve - pressure after the valve affects the valve lift and opening**

- **Balanced Valve - pressure after the valve does not affect the valve lift and opening**

Some Information about Pressure Safety Valves

ADVANTAGES

- simple, low cost and many commercial designs available
- regain normal process operation rapidly because the valve closes when pressure decreases below set value

DISADVANTAGES

- can leak after once being open (O-ring reduces)
- not for very high pressures (20,000 psi)
- if oversized, can lead to damage and failure (do not be too conservative; the very large valve is not the safest!)

Rupture Disk/Burst Diaphragm

ADVANTAGES

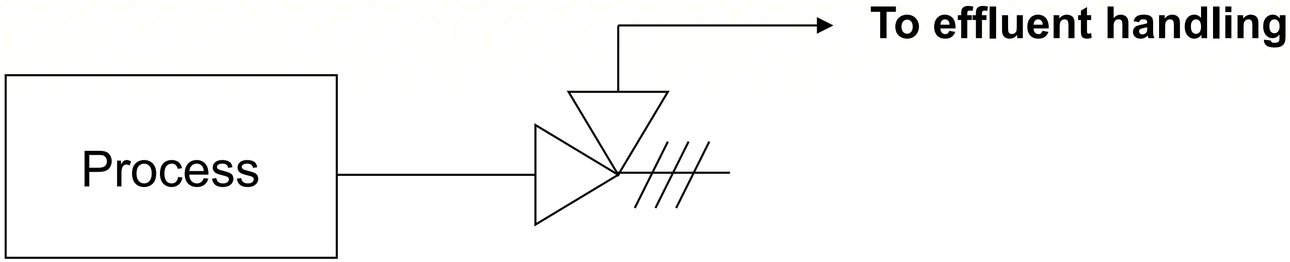
- no leakage until the burst
- rapid release of potentially large volumes
- high pressure applications
- corrosion leads to failure, which is fail safe
- materials can be slurries, viscous, and sticky

DISADVANTAGES

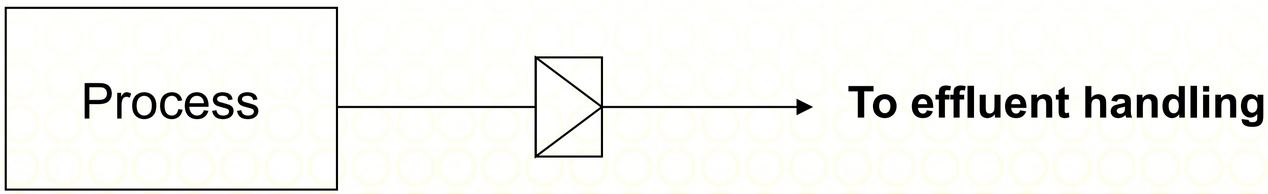
- must shutdown the process to replace
- greater loss of material through relief
- poorer accuracy of relief pressure
- the valve have to be replaced once triggered

Symbols Used in P&I D

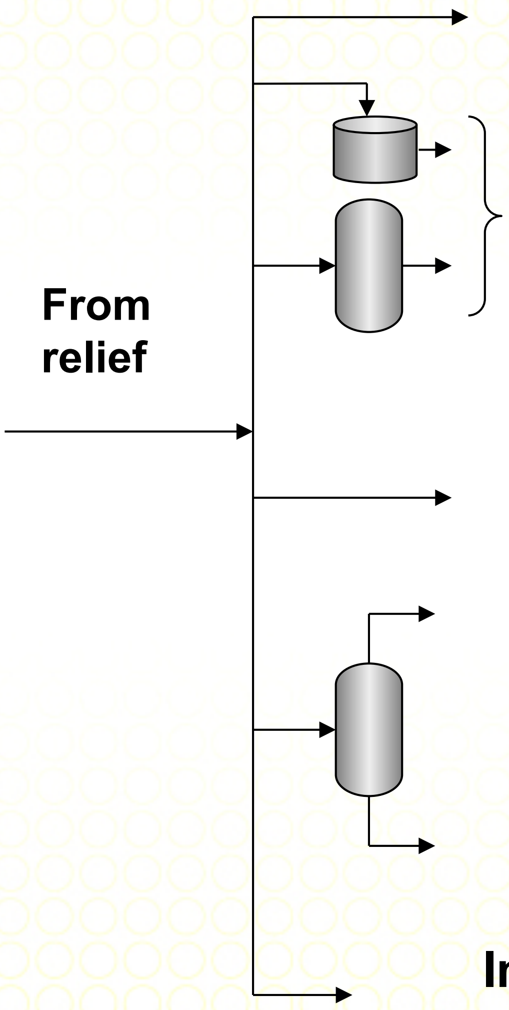
- **Spring-loaded pressure safety valve**



- **Rupture disc**



Materials from relief must be processed or disposed safely



To environment — **e.g. vent steam, air**

Holding for later processing — **Waste water treating**

Recycle to process — **Fuel gas, fuel oil, solvent**

Recover part to process

Immediate neutralization — **Flare, toxic materials**

5. Containment

- Use to moderate the impact of spill or an escape
- Example
  - Bund/dike containment for storage tanks
  - Location of relief valves and vents
  - Diversion to temporary storage /drain system (following breakage of rupture disk)
  - Safety management in containment areas.
  - Containment building (if applicable)

6. Emergency Response Management

- Also used to moderate impact on incidents
- All plants should have ERP (emergency response plan)
  - Assembly, head-counts, evacuation route etc…

MORE INFO ON RELIEF SYSTEM……….

Topic Outline

- Introduction
- Relief concepts
- Definitions
- Location of reliefs
- Relief types

Introduction

Problem

Equipment failures or operator errors may cause increases in process pressure beyond safe levels (i.e. hazardous condition).

If pressure rise too high, they may exceed maximum strength of pipelines or vessels, resulting in rupturing of process equipments,

-causing major releases of toxic or flammable materials

-could lead to contamination and fire (even explosion)

-also plant outages and costly repair

Solution to this problem,

1st line of defense

Inherent safety (keywords: ISAS)

- to prevent the accident in the first place.

2nd line of defense

Better process control (due to process upset, instrument or equipment failure), to maintain the process within the specified operating conditions, avoiding dangerous/high P conditions. Then, alarm system and SIS.

3rd line of defense

Install relief systems to relieve liquids or gases before excessive P build up. Relief system composed of relief device and associated downstream process equipment to safely handle the material ejected.

Note: For Bhopal tragedy, the associated downstream process (scrubber and flare systems) failed to operate.

Relief Concepts

Why need pressure relief systems?

- to protect personnel (workers) from dangers of overpressurizing equipment
- to minimize chemical losses during P upset
- to prevent damage to equipment
- to prevent damage to adjoining property
- to reduce insurance premiums
- to comply with governmental regulations

Relief Method

1. Determine location to place the relief device (also known as pressure relief valve, pressure safety valve, safety valve)
2. Choose type of relief device
3. Develop relief scenario where relief can occur, from this we could determine the flow rate and physical state (single phase (liquid or vapor) or two phase)
4. Acquire data on the relief process (e.g. Physical properties of relief material)
5. Calculation/Sizing of relief device
6. Develop worst case scenario
7. Design relief system

Relief system

Network of components including:

Pipe to relief, relief device, discharge pipelines, knockout drum (blowdown drum or catchtank), scrubber, flare, incinerator, condenser or other types of equipments which assist safe relief.

Definitions related to Relief

- *Set pressure*

  P at which relief device begins to activate.

- *MAWP* (Maximum allowable working pressure)

  Maximum gauge P permissible at top of vessel for a designated T. Sometime called design P. Above this, the vessel might fail/rupture.

- *Operating P*

  The gauge P during normal operation, normally 10% below MAWP.

Normally, Operating P < Set pressure < MAWP

- *Accumulation*.

  P increase over MAWP of vessel during relief process. Expressed as % of MAWP.

- *Overpressure*.

  P increase in vessel over set P during relief process. It expressed as % of set P.

  Note: when set P is at MAWP,

  Overpressure = Accumulation.

- *Backpressure*.

  P at outlet of relief device during relief process resulting from P in the discharge system

Example

Over heating in reactor may cause runaway reaction.

- Consider a reactor with an exothermic reaction. If cooling is lost due to valve failures (no cooling water supplied), reactor T will rise. As T rises the rxn rate increases, leading to increase in heat generation and consequently self-acceleration (runaway rxn).
- P within reactor increases due to increased vapor P of liquid, and/or gas expansion as a result of high T.

Scenario C

If reactor has no relief system and assuming it can withstand full P of runaway!!,

- Let say cooling is lost at t=0.
- P&T rise until reactants are completely consumed
- After reactants completely consumed, reactor cools down and P drops.

Scenario A

If there is a relief device and all vapor phase,

- Let say cooling is lost at t=0.
- When vapor discharged, P drops immediately because only small amount of vapor discharge is required to decrease P.
- P drops until relief valve closed, this P difference called blowdown.

- *Blowdown*

P difference between relief set P and relief reseating P.

Expressed as % of set P.

Scenario B

If there is a relief device and system contains two phase froth (vapor and liquid),

- Let say cooling is lost at t=0.
- When froth is discharged P continues to rise as relief valve opens (note: boiling liquid will produce large volume of vapor).
- The incremental P increase over initial relief P is called overpressure.
- Nature of relieves materials (two phase vapor/liquid or vapor only) must be known because they behave differently

Some questions (what if) asked during review process,

- *what happens if loss of cooling, heating or agitation?*
- *what happens if process is contaminated, or has a mischarge of a catalyst or monomer?*
- *what happens if operator makes an error?*
- *what is the consequence of closing valves (block valves) on vessels or in lines (pipelines) which are filled with liquids and exposed to heat or refrigeration?*
- *what happens if a line fails, e.g. a failure of a high P gas line into a low P vessel?*
- *what happens if unit operation is engulfed in fire?*
- *what conditions cause runaway rxn, and how are relief systems designed to handle those situation?*

Guidelines for specifying relief positions,

- ✓ *all vessels need relief, including reactors, storage tanks, towers, drums.*
- ✓ *blocked-in sections of cool liquid-filled lines which exposed to heat (e.g. sun) or refrigeration need relief.*
- ✓ *positive displacement pumps, compressors, and turbines need reliefs on the discharge side.*
- ✓ *storage vessels need P and vacuum relief to protect against pumping in or out of blocked-in vessel, or against generation of vacuum by condensation.*
- ✓ *vessel steam jackets often rated for low P steam. Reliefs installed in jackets to prevent excessive steam P due to operator error or regulator failure.*

Relief Types

- Factors in selecting relief device are details (types) of the relief systems, process conditions and physical properties of relieved materials.
- Specific devices are chosen for specific application such as for liquids, gases, liquids and gases, solids and corrosive materials .
- Relief materials vented to atmosphere (this is rare due to strict regulations) or vented to containment systems (scrubber, flare, condenser, incinerator etc).

Types of Relief Devices

(i) Spring operated pressure safety valves

Two types:

1. Conventional 2. Balanced Bellows

The adjustable spring tension offset the inlet pressure.

Set P is 10% above the normal operating pressure.

Adjustable screw is securely covered to prevent tempering.

(ii) Rupture discs

i) Spring operated pressure safety valves

a. Conventional

- *Valves open based on the pressure drop across the valve seat*

  The set pressure and the flow is proportional to the pressure drop across the seat (influence by backpressure downstream of the valve).

  Backpressure increase so too the set pressure. Hence, if backpressure increase, flow will decrease.

b. Balanced bellows

- *Designed for process conditions where substantial backpressure existed.*
- *The bellows keeps atmospheric P on spring side, therefore relief opens at the relief set P regardless of process backpressure.*
- *However, the flow rate is still affected by the magnitude of backpressure.*

There are three different application of spring operated pressure safety valves,

(1) *Relief valve* - Primarily for liquid service. Relief valve begins to open at set P. Valve reaches full capacity when P reaches 25% overpressure. Valve closes as P returns to set P.

(2) *Safety valve* - For steam, gas and vapor service. Safety valves pop open when P exceeds set P. This accomplished by using discharge nozzle that directs high velocity material towards the valve seat. After blowdown of excess P, valve reseats at ~4% below set P; hence valve has 4% blow down.

(3) *Safety relief valve* - Used for liquid and vapor service. Safety relief valves function as relief valves for liquids and as safety valves for vapor

ii) Rupture Discs

- *specially designed to rupture at specified relief set P*
- *consist of calibrated sheet of metal designed to rupture at specified P.*
- *can be used alone, in series or parallel to spring loaded relief devices.*
- *made from variety of materials, including corrosion resistant materials.*
- *Once open, will remain open (one-time-use only)*
- *Cheaper than spring-operated valve*
- *Available in much larger sizes than spring-operated valve*

- Frequently installed in series with spring loaded. Why?
  - (a) to protect an expensive spring loaded device from corrosive environment.
  - (b) to give absolute isolation when handling extremely toxic chemicals (spring loaded may weep)
  - (c) to give absolute isolation when handling flammable gases.
  - (d) to protect spring loaded from reactive monomers which may cause plugging.
  - (e) to relieve slurries which may plug spring loaded
- If used before spring loaded relief, P gauge is installed between two devices. This P gauge is an indicator to show when the disc ruptures (such premature ruptures) and need to be replaced

Data for Sizing Relief

For example, sizing relief for reactor with scenario for runaway reaction.

We need physical properties data of chemical involve and reaction data.

Reaction data for runaway rxn could be obtained from equipment call Calorimeter such as:

- Accelerating rate calorimeter
- Reactive system screening tool (RSST)
- Automatic pressure-tracking adiabatic calorimeter (APTAC)
- Vent sizing package (VSP)

Data obtained from this calorimeter:

- maximum self-heat rate
- maximum pressure rate
- reaction onset temperature
- T & P as a function of time

Knockout Drum

- Provided in situations where liquid separation is likely in the waste stream.
- Will collect any liquids that are present in the waste stream prior to entering the flare system.
- Important if substantial cooling of heavy liquids is expected.
- If the liquid is corrosive, use non-corrosive materials of construction.
- A level gauge and drain connections are built into the knockout drum.

Reference

- Crowl, Daniels A. and Louvar, Joseph F., Chemical Process Safety: Fundamentals with Applications, Prentice Hall, 1990, New Jersey, USA.