Chemical Process Safety

Dr. Syeda Sultana Razia
Department of Chemical Engineering, Bangladesh University of Engineering and Technology (BUET), Dhaka -1000
Chemical Process Safety

“To know is to survive and to ignore fundamentals is to court disaster”. 

Japan’s Nuclear Crisis

Bangladesh

- Electricity consumption (2003) 16,196 GW·h

Fukushima I (Daiichi) Nuclear Power Plant

- Annual generation 29,891 GW·h
Nuclear Reactor
What Happened?

- The earthquake caused all operating reactors to automatically shut down (control rods are inserted, which stop the nuclear fission reaction by absorbing neutrons).
- Emergency diesel generators, which started to run the cooling system after the electrical power grid failed, shut down about an hour after the earthquake.
- When cooling fails in a fully operational reactor or shortly after shutdown, the water quickly boils off creating increasing steam pressure in the core containment vessel and exposing the dry fuel assembly to increasing temperatures and radiation. The zirconium metal assembly reacts with the steam to give hydrogen and oxygen, an explosive mix.
Responses to the Threat

First, the plant’s operators attempted to pump cold seawater directly into the reactors to replace the boiled-off coolant water. (Sea water is very corrosive and will undoubtedly damage the metal parts of the reactor, and its complex mixture of contents will also complicate the cleanup. This means to never running it again without a complete replacement of its hardware. As an added precaution, the seawater was spiked with a boron compound in order increase the absorption of neutrons within the reactor).

Next, the bleeding off of some pressure from the reactor vessel in order to lower the risk of a catastrophic failure. (This was also an unappealing option, given that the steam would necessarily contain some radioactivity. Still, it was considered a better option than allowing the container to burst)
Design Errors

- The electrical rooms at these plants are at the basements
- Although the plant was ready for an extreme event, it clearly wasn’t designed with a tsunami in mind—it is simply impossible to plan for every eventuality. However, this seems to be a major omission given the plant’s location. It also appears that the fuel storage areas weren’t nearly as robustly designed as the reactors
Design Errors (cont’d)

- However it is human nature for the less immediate backup systems to be not well designed or maintained as the primary backups, one example is the temporary holding ponds. temporary storage pool for reactor #4 to which the fuel had been transferred while maintenance is performed is a much smaller one near the top the reactor. Unlike the 15-metre deep permanent storage pools

- Another example is that the backup portable generators – planned for when the batteries were exhausted – which is the 3rd (or 4th) backup for power generation – had the wrong connectors and so could not be used
Definitions

- **Safety/loss prevention**: the prevention of accidents through the use of appropriate technologies to identify the hazards of chemical plant and eliminate them before an accident occurs.

- **Hazard**: a chemical or physical condition that has the potential to cause damage to people, property, or the environment.

- **Risk**: a measure of human injury, environmental damage, or economic loss in terms of both the incident likelihood and the magnitude of loss and injury.
Safety Programs

☐ System
☐ Attitude
☐ Fundamentals
☐ Experience
☐ Time
☐ You
Safety Programs cont’d

- A **Good** safety program identifies and eliminates existing safety hazards
- An **Outstanding** safety program has management system that prevent existence of safety hazards
AIChe Code of Professional Ethics: Fundamental Principles

- Engineers shall uphold and advance the integrity, honor, and dignity of the engineering profession by
  - Using their knowledge and skill for the enhancement of human welfare
  - Being honest and impartial and serving with fidelity the public, their employers and clients
  - Striving to increase the competence and prestige of the engineering profession
AIChe Code of Professional Ethics: Fundamental Canons

☐ Engineers shall hold paramount the safety, health and welfare of the public in the performance of their professional duties.

☐ Engineers shall perform services only in areas of their competence.

☐ Engineers shall issue public statements only in an objective and truthful manner.

☐ Engineers shall continue their professional development throughout their careers and shall provide opportunities for the professional development of those engineers under their supervision.
## Types of Chemical Plant Accidents

<table>
<thead>
<tr>
<th>Type of accidents</th>
<th>Probability of occurrence</th>
<th>Potential for fatalities</th>
<th>Potential for economic loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire</td>
<td>High</td>
<td>Low</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Explosion</td>
<td>Intermediate</td>
<td>Intermediate</td>
<td>High</td>
</tr>
<tr>
<td>Toxic release</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

![Pie chart showing the distribution of different types of accidents.

- Fires: 31%
- Explosions: 30%
- Vapor Cloud Explosions: 36%
- Other: 3%]
Statistics


Acceptable Risk & Public Perceptions

- We cannot eliminate risk entirely
- In a single Chemical Process plant the risk becomes too high because of multiple exposure to several processes
- Modern site layout requires sufficient separation of plants within site to minimize multiple exposure
- Public perception about hazards of chemicals can be confusing and may not reflect the real situation
Case History 1: (Washington DC, Manufacturing Chemists’ association)

- Static Electricity: Tank car loading explosion
  - Two plant operators were filling a tank car with vinyl acetate. After few seconds the contents of the tank exploded, one operator died from fractured skull and body burns
  - Caused by a static spark jumped from the steel nozzle to the tank car
Chemical Reactivity

Bottle of isopropyl ether; A chemist twisted the cap of a bottle of isopropyl ether to open it. As the cap broke loose, the bottle exploded. The man died due to massive internal hemorrhage.

Caused by rapid decomposition of peroxides, which formed in the ether while the bottle sat in storage.
Case History 3: (Washington DC, Manufacturing Chemists’ association)

- System Design
  - Ethylene oxide explosion: A process storage tank contained 6500 gal of ethylene oxide. It was accidentally contaminated with ammonia. The tank ruptured and dispersed ethylene oxide into the air. A vapor cloud was formed and immediately exploded. One person was killed and nine were injured; property losses $16.5 million
  - Lack of design protection to prevent back up of ammonia into the storage tank.
Case History 4: (Washington DC, Manufacturing Chemists’ association)

- System Procedure
  - Man working in a Vessel: two maintenance workers were replacing part of a ribbon in a large ribbon mixer. The main switch was left energized, the mixer was stopped with one of three start-stop buttons. The operator by mistake pushed one of the start stop button, the mixer started and the mechanic inside was killed.
Example of Disaster: Bhopal, India (December 3, 1984)

- Plant Location: Madhya Pradesh, central India; nearest inhabitants were 1.5 miles away, but a shanty town grew nearby.
- Produced Pesticides; owned by Union Carbide and partially owned locally
- Intermediate compound methyl iso-cyanate (MIC): reactive, toxic, volatile, flammable and vapor heavier than air.
- MIC unit was not operating because of labor dispute
Example of Disaster cont’d

☐ Accident:
  ■ Storage tank containing large amount of MIC became contaminated by water, heated by reaction; vapor traveled through pressure relief system into a scrubber and flare system that was not operating
  ■ 25 tons toxic MIC vapor released, spread to the adjacent town killing over 2000 civilians and injuring 20,000 more. No plant workers were killed.

☐ Recommendation:
  ■ Alternative reaction scheme or redesigning of the process with reduced inventory of MIC (less than 20 pounds)
Hazard Identification

- What are the hazards?
- What can go wrong?
- What are the chances?
- What are the consequences?
Hazard Identification and Risk Assessment Procedure

1. System description

2. Hazard identification

3. Scenario identification

   - Accident probability
   - Accident consequences

4. Risk determination

   - Risk and/or hazard acceptance
   - Build and/or operate system

   - Modify
     1. process or plant
     2. process operation
     3. emergency response
     4. other

   - no

   - yes
Hazard Identification Methods

- Process hazards check lists
- Hazard surveys
- Hazards and operability (HAZOP) studies
- Safety review
- What-if analysis
Example: DAP Process

Example

A proposed continuous process is shown in Figure 6.1. In this process, a phosphoric acid solution and an ammonia solution are provided through flow control valves to an agitated reactor. The ammonia and phosphoric acid react to form diammonium phosphate (DAP), a nonhazardous product. The DAP flows from the reactor to an open-top storage tank. Relief valves are provided on the storage tanks and the reactor with discharges to outside of the enclosed work area.

If too much phosphoric acid is fed to the reactor (compared to the ammonia feed rate), an off-specification product is created, but the reaction is safe. If the ammonia and phosphoric acid flow rates both increase, the rate of energy release may accelerate, and the reactor, as designed, may be unable to handle the resulting increase in temperature and pressure. If too much ammonia is fed to the reactor (as compared to the normal phosphoric acid feed rate), unreacted ammonia may carry over to the DAP storage tank. Any residual ammonia in the DAP tank will be released into the enclosed work area, causing personnel exposure. Ammonia detectors and alarms are provided in the work area.
Hazards and Operability (HAZOP) Studies

- Begin with a detailed flow sheet and break the flow sheet into a number of process units
- Choose a study node (Vessel, line etc.)
- Pick a process parameter: flow, level, T, P, concentration, pH, viscosity, reaction etc
- Apply a guide word to suggest possible deviation
- If the deviation is applicable determine possible causes and note any protective system
- Evaluate the consequences
- Recommend action
- Record all information
### HAZOP Analysis Worksheet - I

**Team:** HAZOP Team #3  
**Meeting Date:** 6/27/81  
**Drawing Number:** 70-OBP-57100  
**Revision Number:** 3

<table>
<thead>
<tr>
<th>Item No.</th>
<th>Deviation</th>
<th>Causes</th>
<th>Consequences</th>
<th>Safeguards</th>
<th>Actions</th>
</tr>
</thead>
</table>
| 4.0      | Line - Phosphoric acid feed line to the DAP reactor. Deliver acid feed to reactor at a rate of x gpm and y psig (dwg: Figure 6.6) | No feed material in the phosphoric acid storage tank  
Flow indicator fails high  
Operator sets phosphoric acid flow rate too low  
Phosphoric acid feed line control valve B fails closed  
Plugging of line  
Leak or rupture of line | Unreacted ammonia in the reactor carried over to the DAP storage tank and released to the enclosed work area | Periodic maintenance of valve B  
Ammonia detector and alarm | Consider adding an alarm/shutdown of the system for low phosphoric acid flow to the reactor  
Ensure periodic maintenance and inspection for valve B is adequate  
Ensure adequate ventilation exists for enclosed work area and/or consider using an enclosed DAP storage tank |
<table>
<thead>
<tr>
<th>Item No.</th>
<th>Deviation</th>
<th>Causes</th>
<th>Consequences</th>
<th>Safeguards</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.10</td>
<td>Loss of agitation</td>
<td>Agitator motor fails</td>
<td>Unreacted ammonia in the reactor carried over to the DAP storage tank and released to the enclosed work area</td>
<td>Ammonia detector and alarm</td>
<td>Consider adding an alarm/shutdown of the system for loss of agitation in the reactor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agitator mechanical linkage fails</td>
<td></td>
<td></td>
<td>Ensure adequate ventilation exists for enclosed work area and/or consider using an enclosed DAP storage tank</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator fails to activate the agitator</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example: Cooling

Figure 10-8  An exothermic reaction controlled by cooling water.
# HAZOP Analysis Worksheet

## Hazards and Operability Review

**Project name:** Example 10-2  
**Date:** 1/1/93  
**Completed:** No action  
**Page 1 of 2**

**Process:** Reactor of Example 10-2

**Section:** Reactor shown in Example 10-2  
**Reference drawing:** Figure 10-8

<table>
<thead>
<tr>
<th>Item</th>
<th>Study node</th>
<th>Process parameters</th>
<th>Deviations (guide words)</th>
<th>Possible causes</th>
<th>Possible consequences</th>
<th>Action required</th>
<th>Assigned to</th>
</tr>
</thead>
</table>
| 1A   | Cooling coils | Flow | No | 1. Control valve fails closed  
2. Plugged cooling coils | 1. Loss of cooling, possible runaway | 1. Select valve to fail open  
2. Install filter with maintenance procedure  
3. Check and monitor reliability of cooling system | DAC 1/93 |
| 1B   | High       |         | 3. Cooling water service failure  
4. Controller fails and closes valve  
5. Air pressure fails, closing valve  
1. Control valve fails open | 2. " | DAC 1/93 |
| 1C   | Low        |         | 2. Controller fails and opens valve  
1. Partially plugged cooling line  
2. Partial water supply failure  
3. Control valve fails to respond | 1. Diminished cooling, possible runaway  
2. " | DAC 2/93 |
| 1D   | As well as, part of, reverse | | 1. Contamination of water supply  
1. Covered under 1C  
1. Failure of water source resulting in backflow | 1. Not possible here  
1. Loss of cooling, possible runaway | DAC 2/93 |
| 1E   | Other than, sooner than, later than | | 2. Backflow due to high backpressure  
1. Not considered possible  
1. Cooling normally started early  
1. Operator error | 1. None  
1. Temperature rises, possible runaway | DAC 2/93 |
| 1F   | Low        | | | | | |
| 1G   | Where else, sooner than, later than | | | | | |
| 1H   | Temp.      | | | | | |
| 1I   | Low        | | | | | |
| 1J   | Low        | | | | | |
| 1K   | High       | | | | | |
| 1L   | Low        | | | | | |
| 2A   | Stirrer    | Agitation | No | 1. Stirrer motor malfunction  
2. Power failure | | 1. Interlock between cooling flow and reactor feed  
1. None—controller handles  
1. Cooling system capacity limited, temp. increases  
1. No mixing, possible accumulation of unreacted materials  
2. Monomer feed continues, possible accumulation of unreacted materials  
1. None | JW 1/93 |
| 2B   | More       | | | 1. Stirrer motor controller fails, resulting in high motor speed | | | |

**Reply date:**
What-if Analysis

- Begin with process description, drawings and operating procedures
- Identify hazards by applying the words “what-if” to a number of areas of investigation
- Find out
  - the potential consequences
  - how to solve any problems
- Recommend action
- Record all information
## What-if Analysis Worksheet

### Table 6.9 Sample Page from the What-If Analysis Table for the DAP Process Example

**Process:** DAP Reactor  
**Topic Investigated:** Toxic Releases  
**Analysts:** Mr. Safety, Ms. Opera, Mr. Design  
**Date:** 05/13/95

<table>
<thead>
<tr>
<th>What-If</th>
<th>Consequence/Hazard</th>
<th>Safeguards</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>the wrong feed material is delivered instead of phosphoric acid?</td>
<td>Potentially hazardous phosphoric acid or ammonia reactions with contaminants, or production of off-specification product</td>
<td>Reliable vendor</td>
<td>Ensure adequate material handling and receiving procedures and labeling exist</td>
</tr>
<tr>
<td>the phosphoric acid concentration is too low?</td>
<td>Unreacted ammonia carryover to the DAP storage tank and release to the work area</td>
<td>Reliable vendor</td>
<td>Verify phosphoric acid concentration before filling storage tank</td>
</tr>
<tr>
<td>the phosphoric acid is contaminated?</td>
<td>Potentially hazardous phosphoric acid or ammonia reactions with contaminants, or production of off-specification product</td>
<td>Plant material handling procedures</td>
<td>Ensure adequate material handling and receiving procedures and labeling exist</td>
</tr>
<tr>
<td>valve B is closed or plugged?</td>
<td>Unreacted ammonia carryover to the DAP storage tank and release to the work area</td>
<td>Reliable vendor</td>
<td>Alarm/shutoff of ammonia (valve A) on low flow through valve B</td>
</tr>
<tr>
<td>too high a proportion of ammonia is supplied to the reactor?</td>
<td>Unreacted ammonia carryover to the DAP storage tank and release to the work area</td>
<td>Reliable vendor</td>
<td>Alarm/shutoff of ammonia (valve A) on high flow through valve A</td>
</tr>
<tr>
<td></td>
<td>Ammonia detector and alarm</td>
<td>Ammonia detector and alarm</td>
<td></td>
</tr>
</tbody>
</table>
Risk Assessment

- Risk assessment includes
  - Incident identification: describes how an accident occurs and analyses probabilities
  - Consequence analysis: describes the expected damage, including loss of life, damage to environment or capital equipment and days outage
Fault Trees Method

- Fault trees are a deductive method for identifying ways in which hazards can lead to accidents.
- It started with a well-defined accident, or top event, and works backward toward the various scenario that can cause the accident.
Example: Chemical Reactor with an Alarm

Figure 11-5 A chemical reactor with an alarm and an inlet feed solenoid. The alarm and feed shutdown systems are linked in parallel.
Fault Trees

![Fault Tree Diagram]

- **Top Event**: Overpressuring of Reactor
  - **Probability**: P = 0.0702
  - **Reliability**: R = 0.9298

- **Failure of Alarm Indicator**
  - **Probability**: P = 0.1648
  - **Reliability**: R = 0.8352

- **Failure of Emergency Shutdown**
  - **Probability**: P = 0.4258
  - **Reliability**: R = 0.5742

- **Pressure Switch 1 Failure**
  - **Probability**: P = 0.13
  - **Reliability**: R = 0.87

- **Pressure Indicator Light Failure**
  - **Probability**: P = 0.04
  - **Reliability**: R = 0.96

- **Pressure Switch 2 Failure**
  - **Probability**: P = 0.13
  - **Reliability**: R = 0.87

- **Solenoid Valve Failure**
  - **Probability**: P = 0.34
  - **Reliability**: R = 0.66
Aids for Recommendation

- Control plant modifications
- User friendly designs
- Block valves
- Double block and bleed
- Preventive maintenance
- Analyzers
Figure 12-2  A block valve arrangement used to prevent leakage from the connecting hose. If the flow at both ends of the hose is not identical, the block valves are closed.
Figure 12-3  A double block and bleed arrangement used to prevent reactant from entering reactor vessel.
References

- Guidelines for Hazard Evaluation Procedures (second edition with worked examples)
  - Center for Chemical Process Safety, AIChE

- Chemical Process Safety: Fundamentals with applications
  - Daniel A. Crowl and Joseph F. Louvar