SAFETY LAYERS
AND LAYER OF PROTECTION ANALYSIS
(LOPA)

North Jersey Section AIChE
September 2020
WHO AM I?

- Peter Sibilski, P.E., CEM, FAIChe
- Plant Manager, Pharmetic Manufacturing Co., LLC
- B.S., Chemical Engineering - NJIT
- MBA, Technology Management - University of Phoenix
- Work experience includes:
  - Diamond Shamrock – specialty chemicals
  - Occidental Chemical – specialty chemicals
  - Henkel Chemical – specialty chemicals
  - Olin Hunt – microelectronics chemicals
  - EI Associates – A/E consulting
  - BOC Gases – industrial gases
  - Schering-Plough - pharmaceuticals
  - ALZO International, Inc. – specialty chemicals
Information presented on these slides was obtained (with permission) from:

- **Consider the Role of Safety Layers in the Bhopal Disaster** – Ronald J. Willey, P.E., CEP Magazine, December 2014

- …as well as over 30 years of experience in the chemical process industry!
BHOPAL DISASTER

[Map of India with Bhopal marked]

[Bhopal plant damage images]

North Jersey Section, AIChE
THE PLANT

- Owned by Union Carbide India, Ltd (UCIL)
  - Joint venture of UC and a group of Indian government-controlled institutions
  - Located about 2 miles north of Bhopal railway station
- Agricultural Products Division of UCIL operated the plant
  - Manufactured fungicides, miticides, herbicides and insecticides
  - Accounted for just over 8% of UCIL sales
- Opened (new) in 1970 initially only blending pesticides
- Backward integrated over time, with methyl isocyanate (MIC) production beginning in 1980
- Capacity was 5,250 metric tons (~ 11.6 million lbs) MIC / year
- Bunker constructed, containing three 15,000 gallon storage tanks for MIC
METHYL ISOCYANATE AT A GLANCE

Manufacture

Methyl isocyanate is usually manufactured by the reaction of monomethylamine and phosgene. For large scale production, the mixture is condensed, leaving one mole of hydrogen chloride.

\[ \text{Cl}_2 + \text{H}_3\text{C}-\text{NH}_2 \rightarrow \text{H}_3\text{C} = \text{NH} - \text{Cl} + \text{HCl} \]

The methyl isocyanate is obtained by treating the MCC with a tertiary amine, such as N,N-dimethylaniline, or using distillation techniques.[13]

\[ \text{H}_3\text{C} = \text{NH} - \text{Cl} \rightarrow \text{H}_3\text{C} = \text{N} = \text{C} = \text{O} + \text{HCl} \]

Methyl isocyanate is also manufactured from N-methylformamide and air. In the latter process, it is immediately used in the manufacture of methanol.[14] Other manufacturing methods have been reported.[15][16]

---

North Jersey Section, AIChE
THE STORAGE TANK BUNKER

- Design intent was for Tanks 610 and 611 to each store ½ capacity (7,500 gallons) of MIC

- Tank 619 was reserve capacity for excess and/or O.O.S. MIC

- Tank 610 was the source of the release
THE STORAGE TANK PFD

Figure 2. The tanks were equipped with refrigeration units to maintain storage temperatures below 15°C and nitrogen blanketing to prevent ignition of the MIC. Source: Adapted from Ref. 6.
THE VENT GAS SCRUBBER & FLARE TOWER

Figure 3. A scrubbing system downstream from the tank was designed to capture toxic emissions and vent them to a flare tower. Source: Adapted from Ref. 7.
7 LAYERS OF PROTECTION TYPICALLY EMPLOYED IN CPI

1st Layer: Process Design
2nd Layer: Basic Control Systems and Alarms
3rd Layer: Critical Alarms, Manual Intervention
4th Layer: Automated Safety Instrumented System
5th Layer: Relief Devices
6th Layer: Containment of Releases
7th Layer: Plant’s Emergency Response Procedures

“8th Layer”: Community Response – when it gets to this level, it’s typically catastrophic

IMPORTANT: Each layer must be independent of the others!
LOPA techniques evolved from the late 1980’s to the 1990’s to evaluate major layers that can mitigate the injury & damage from an event like a fire, explosion or release.

LOPA is a holistic approach, identifying major safeguards, categorizing them, determining if they are dependent or independent, and assessing their ability to perform on demand.

LOPA is a semi-quantitative analysis tool to evaluate whether adequate mitigation exists for a particular process safety incident, (i.e.; Initiating Event, or I.E.)

LOPA estimates the effectiveness of existing major layers of protection to prevent/mitigate an I.E., the frequency of which is denoted “IEF”

LOPA is not a complete event-tree analysis.

North Jersey Section, AIChE
LOPA - continued

- In a LOPA analysis, only two outcomes exist:
  - The protective measure works when it is needed, or
  - The protective measure does not work when it is needed

- These two potential outcomes can be characterized by:
  - A probability to work on demand (PWD), or
  - A probability to fail on demand (PFD)

- The sum of these probabilities = 1.0 for each independent protection layer (IPL)

- The key equation of the LOPA analysis therefore is:

\[ f_i^c = IEF_i \times PFD_{i1} \times PFD_{i2} \times \ldots \times PFD_{ij} \]
LOPA - continued

\[ f_i^c = IEF_i \times PFD_{i1} \times PFD_{i2} \times \ldots \times PFD_{ij} \]

- \( f_i^c \) = the frequency of the consequence occurring for scenario “i” per unit time \( (time^{-1}) \)

- \( f_i^c \) = a relative number used to compare different layers and scenarios

- \( IEF_i \) = the frequency of the initiating event for scenario “i” per unit time \( (time^{-1}) \)

- \( PFD_{ij} \) = the probability of failure on demand of the independent protection layer “j” for scenario “i”
SCENARIO:
- Major release of MIC vapor into surrounding community

INITIATING EVENT: (possibilities)
- Storage tank leak
- Wall of tank fails (e.g.; an explosion)
- Relief system fails

IDENTIFY THE MOST LIKELY EVENT:
- Contamination of storage tank contents (The actual event that initiated the Bhopal disaster was traced to the entry of ~ 500 kg of water into Tank 610)

IDENTIFY THE FREQUENCY OF THE INITIATING EVENT (IEF):
- This may be known, or it may need to be estimated
  » The MIC plant opened in 1980 and the initiating event occurred 4.8 yrs after the plant began operating: $\text{IEF} = 1 \text{ event} / 4.8 \text{ yrs} = 0.21 \text{ yr}^{-1}$
LAYERS OF PROTECTION DESIGNED INTO STORAGE TANK 610

**LAYER 1: Corporate Design Intent**

- Two product storage tanks, (Tanks 610 & 611) each sized for twice the required volume, plus a third tank (Tank 619) for excess and off-spec product
- Tanks were equipped with level control indicators connected to alarms in the Control Room
- Operating training was also a part of this first layer

**CALCULATE / ESTIMATE THE PFD FOR THIS LAYER:**

- It would be reasonable to estimate the probability for failure on demand for these measures as 1 failure every 10 years, or \( PFD_{11} = 0.1 \)
LAYERS OF PROTECTION DESIGNED INTO STORAGE TANK 610

● LAYER 2: Basic Controls

  – The tanks were equipped with a temperature control system – an external refrigeration system was used to maintain the tank temperature at less than 15°C

● CALCULATE / ESTIMATE THE PFD FOR THIS LAYER:

  – It would be reasonable to estimate the probability for failure on demand for this measure as 1 failure every 10 years, or $PFD_{12} = 0.1$
LAYERS OF PROTECTION DESIGNED INTO STORAGE TANK 610

- LAYER 3: Critical Alarms and Manual Intervention
  - The tanks were equipped with a temperature and level indicators that would sound an alarm and flash warning lights on a Control Room panel.
  - The plant’s safety manual stated:
    » “If the methyl isocyanate tank becomes contaminated or fails, transfer part or all of the contents to the empty, standby tank” (1)

- CALCULATE / ESTIMATE THE PFD FOR THIS LAYER:
  - This layer depends on a human response to an abnormal condition, which under the best of circumstances has a \( PFD_{13} = 0.1 \) (2)

---


LAYERS OF PROTECTION DESIGNED INTO STORAGE TANK 610

- LAYER 4: Safety Instrumented System (SIS) or Emergency Shutdown Device (ESD)
  - The MIC plant was not equipped with either an SIS or an ESD

- CALCULATE / ESTIMATE THE PFD FOR THIS LAYER:
  - \( PFD_{14} = 1.0 \)
LAYERS OF PROTECTION DESIGNED INTO STORAGE TANK 610

● LAYER 5: Relief Devices
  – The relief system consisted of a rupture disc, a relief valve, and a flare system, in series.
    » NOTE: Although the NaOH scrubber was also part of the relief system, it was designed for small releases and therefore does not affect the scenario of a major release of MIC

● CALCULATE / ESTIMATE THE PFD FOR THIS LAYER:
  – The overall PFD for this combination of devices is $PFD_{15} = 0.1$
LAYERS OF PROTECTION DESIGNED INTO STORAGE TANK 610

- LAYER 6: Dike
  
  - The plant did not have a secondary containment dike.
    
    **NOTE:** Even if a dike were present, it’s PFD would = 1.0, MIC is extremely volatile and temperatures in central India can exceed the 39°C boiling point of MIC. Vapors would evolve at deadly concentrations, making a containment dike meaningless.

- CALCULATE / ESTIMATE THE PFD FOR THIS LAYER:
  
  - $PFD_{16} = 1.0$
LAYERS OF PROTECTION DESIGNED INTO STORAGE TANK 610

- LAYER 7: Plant Emergency Response
  - Some plant personnel were trained in emergency response and attempted to respond.

- CALCULATE / ESTIMATE THE PFD FOR THIS LAYER:
  - As with Layer 3, this layer depends on a human response to an abnormal condition, which under the best of circumstances has a $PFD_{13} = 0.1$ \(^{(2)}\)

---

FREQUENCY OF OCCURRENCE CALCULATION

\[ f_i^c = IEF_i \times PFD_{i1} \times PFD_{i2} \times \ldots \times PFD_{ij} \]

- \[ f_1^c = IEF_1 \times [PFD_{11} \times PFD_{12} \times PFD_{13} \times PFD_{14} \times PFD_{15} \times PFD_{16} \times PFD_{17}] \]

- \[ f_1^c = (0.1 \text{ yr}^{-1}) \times [0.1 \times 0.1 \times 0.1 \times 1.0 \times 0.1 \times 1.0 \times 0.1] = 1 \times 10^{-6} \text{ yr}^{-1} \]

In other words – if everything was adequately designed and functioning properly, the frequency of this catastrophic release occurring would be:

1 major release in a million years!

So why, then, did this event occur at all?

**Answer:** Because all of the layers were compromised, and therefore the PFD for each layer was = 1.0
The operating instructions specified, “**Do not overfill the tank beyond 50% full with MIC**”.
- Someone within operating supervision made the decision to fill the tank to 85% of capacity

**LESSON(S):**
- **MIC** was an intermediate. What you don’t have in inventory cannot leak, catch fire or otherwise cause a problem.
- Design the plant to produce and use intermediates on demand.
The refrigeration system installed to remove the exothermic heat of reaction within the storage tank was disabled by plant management. *This was portrayed as a cost-saving measure as plant management was under pressure to cut costs to avoid plant closure.*

**LESSON(S):**

- Management continually looks for ways to reduce costs. Engineers need to communicate that cost reductions should not be undertaken for critical safety systems.
- Evaluate the removal of any safety systems through an MOC analysis to understand the implications.
ANALYSIS - Layer 3: Instrumentation & Manual Intervention

- The plant had high-temperature and high-level indicators and alarms to alert personnel
  - Operators were aware of the rising pressure and temperature in Tank 610; however, there is no record of a manual intervention to transfer material to Tank 619

- LESSON(S):
  - This layer relies on human factors and requires people to take corrective action in an emergency
  - Training exercises that simulate the proper corrective action(s) should be developed within the plant and practiced by operators.
ANALYSIS - Layer 4: Automation

- No Safety Instrumented System (SIS) or Emergency Shut-down Device (ESD) was evident in the design of the Bhopal plant
  - *For example, there was no automated device that might quench a runaway reaction with the storage tank*

- LESSON(S):
  - *Under the right conditions SIS and ESD can have a PFD = 0.01*
  - *It is important that the SIS and/or ESD be completely independent and work without any human intervention.*
ANALYSIS - Layer 5: Relief System

- The rupture disc followed by the relief valve worked on demand and the RVVH had sufficient capacity, preventing what could have been a even more catastrophic explosion
  - However, the relief system failed because the flare system was out of service awaiting replacement of a 4-foot section of corroded pipeline. The material in the RVVH had nowhere to go but into the air.

- LESSON(S):
  - Are any of your safety systems out of service awaiting repair?
  - If so, is there a sense of urgency to make the repair so that the safety systems are available to do their job on demand?
ANALYSIS - Layer 6: Diking

- The existence of a dike is irrelevant, since this was a toxic gas release
  - *Diking around the storage tanks would not have affected the outcome of this disaster.*

- LESSON(S):
  - *Do your liquid storage tanks have diking and has it been inspected recently?*
  - *If not equipped with a dike or catch basin would you be concerned if a major release were to occur?*
A few operators tried spraying water on the gas plume leaving the scrubber
  - The hoses were insufficiently pressurized and the 100-foot-high stream could not reach the plume, which was exiting at 120 feet.

LESSON(S):
  - Emergency response must be practiced. Mock scenarios need to be run through so things like low water pressure will be discovered beforehand
  - Should every employee at your facility have the authority to shut down the plant if a potentially unsafe event appears to be happening?
IN CONCLUSION...
“There is no expedient to which a man will not resort to avoid the real labor of thinking.”

Sir Joshua Reynolds