Introduction to Process Safety & Risk Assessment

Protection Layers

Ahmad Shafaghi

University of West Indies

October 4, 2013
Seminar Contents

- Overview of Trinidad & Tobago Process Industry
- Basic Concepts and Process Safety
- Texas City Disaster (Video)
- Protection Layers
- Hazard Impacts
- Risk Assessment
Incident Anatomy

- Incidents are the result of a series of events.
- An incident starts with an initiating event; categories are equipment failure, human error, external causes or events from upstream or downstream.
- System is designed to tolerate disturbances up to certain values (safe upper and lower operating limits).
- If the disturbances either not controlled or cannot be controlled (due to their magnitudes) then a hazardous condition can occur.
- The system protection layers are designed to prevent further escalation of the event within the system.
- If the protection layers fail then an incident happens.
Protection Layer Types

- Functionally they are in a layer arrangement
- Dependency:
  - Those that are independent of other layers and initiating events called Independent Protection Layer (IPL)
  - Those that are interdependent of other layers, called Non-independent.
- Instrumented:
  - Procedural
  - Engineered
- Some are designed to act before the incident – Preventive (or Preventative)
- Some are designed to reduce the intensity of the incident - Mitigation
Protection Layers Preventing Incidents

Non-IPLs  Independent Protection Layers (IPLs)

Initiating Events  Protection Layers

Incident
Ahmad Shafaghi
Layer of Protection Classification

- Incident Prevention layers
- Incident Mitigation Layers
Prevention Layers

- **Process Control Layer** – The Basic Process Control System BPCS, which provides significant safety through proper design of process control.
- **Critical Alarms and Operator Intervention** – This layer of protection is also provided by the control system and the operators.
- **Safety Instrumented System (SIS)** – This safety system is independent of the process control system. It has separate sensors, valves and logic system.
- **Active Protective System** – This layer may include pressure relief valves and rupture disks designed to provide a relief point that prevents a rupture.
Mitigation Layers

- **Passive Protection** – It may consist of a dike or other passive barrier that serves to contain a fire or channel the energy of an explosion in a direction that minimizes the spread of damage.

- **Emergency Response System of the Facility** – When an incident was not mitigated by Passive Protection System an emergency response system must be to minimize the harms such as facility damage, operator/public injuries or loss of life. This system may include evacuation plans and fire fighting facilities.

- **Emergency Response System of the Community** – The local government with the assist of the process facilities must develop a plan to warn, evacuate and shelter the community in case of major incidents.
Protection Layer Strength

Initiating Event -> First Protection Layer

Protection Layer Capable?
- Yes
- No: Protection Layer Not Capable -> Second Protection Layer

Protection Layer Available?
- Yes
- No: Protection Layer Not Available -> Second Protection Layer

Protection Layer Response Fast?
- Yes
- No: Protection Layer Not Fast Enough -> The Process Continues for all Protection Layers

Incident Prevented
What is Layer of Protection Analysis (LOPA)?

- LOPA is a semi-quantitative risk assessment.
- LOPA is a systematic method for assessing the adequacy of protection layers for hazardous events.
- This is a follow-up to a hazard analysis (e.g., HAZOP) where hazardous events, their causes and existing protections have been identified.
- Using a risk targets the amount of risk reduction needed is determined.
- Risk reduction can be achieved by addition or enhancement of layers of protection.
Layer of Protection Analysis (Semi-Quantitative Risk Assessment)

1. **Selected Scenarios for LOPA**
2. **Select a Scenario (Event)**
3. **Determine Initiating Event Frequency (ICL)**
4. **Identify and Calculate Modifiers**
5. **Identify IPL Probability of Failure on Demands (PFDs)**
6. **Calculate IEL for the Selected Event**
7. **Other Scenario Result in Same Consequence?**
   - Yes
   - No
8. **Sum All IELs**
9. **Target Mitigated Event Likelihood (TMEL)**
10. **Is \( \Sigma IEL \leq TMEL? \)**
11. **No Additional Layer Needed**
12. **Calculate Risk Reduction Factor & Upgrade Layer**

Ahmad Shafaghi
Semi-Quantitative Risk Calculation - I

\[ IEL = ICL \times PFD_1 \times PFD_2 \ldots PFD_n \times \text{Modifiers} \]

Where,

- \( ICL \) = Initiating Event Likelihood (frequency\(^\dagger\))
- \( PFD_i \) = Probability of Failure on Demand of IPL “i”

Modifiers = Conditional Probabilities of certain factors, e.g., exposure and ignition

- \( IEL \) = Intermediate Event likelihood (frequency)

If

\( IEL \leq TMEL \); Then no risk reduction is required.

Where,

- \( TMEL \) = Target Mitigated Event Likelihood (frequency)

\(^\dagger\) Frequency \( \equiv \) Number of events per a period of time of cycle, e.g., a year
If \( \text{Sum IELs} \geq \text{TMEL} \), then how much risk reduction is necessary?

This will depend on the “PFD gap”, which is determined as follows:

\[
PFD \text{ Gap} = \frac{\text{TMEL}}{\text{Sum of IELs}}
\]

&

\[
\text{RRF} = \frac{1}{PFD \text{ Gap}}
\]

Where,

RRF = Risk Reduction Factor

Example:

If \( \text{Sum IEL} = 10^{-4} \), but \( \text{TMEL} \) is \( 10^{-5} \), then \( \text{RRF} = 10 \)

Therefore there is a need to upgrade the IPLs.
Once the IELs are calculated, then the calculated value is compared with the target mitigated event likelihood (TMEL) of the corresponding consequence severity.

The IEL value could be the sum of the intermediate event likelihood resulting the same consequence.

That is,

\[
\text{Sum of IELs} \leq \text{TMEL}
\]

If this relationship stands then no reduction in risk is necessary.
Failure of Layers Protection at Texas Refinery Incident

- The operator did not follow startup procedure (initiating event)
- Basic process control system failed
  - Splitter level control system malfunction
  - Pressure transmitter malfunction
- Critical alarms and operator intervention failed
- No emergency shutdown devices were in place
- Relive valves failed
- Blowdown system failed
- Safe distance between process units and trailers was not enforced
Representation of Layer of Protection Failure at Texas Refinery Incident

- Fail to start up properly
- Basic Process
- Alarms/Operator Response
- Relief Valve
- Blowdown System
- Fire and Explosion
- Safe Distance to Portable Offices
- 15 People Died

Ahmad Shafaghi