CE 400 / CE 500

Process Safety Management

Lecture 29 Layer of Protection Analysis Part II

Instructor: David Courtemanche

University at Buffalo
Department of Chemical and Biological Engineering
School of Engineering and Applied Sciences

LOPA

- A semi-quantitative method to Risk Analysis
- Start with a specific scenario
  - A specific initial failure leads to a specific undesired outcome
- Choose a Risk Goal to obtain
  - Example – Obtain a Risk Level of III
- Have a set of Rules to Follow
  - Each company must generate their own process, but there are generally accepted guidelines
- Document the Process
  - Each company must generate their own format, but there are generally accepted guidelines

Cause / Consequence Pairs

- A LOPA scenario has a unique initiating event/loss event pair
- Each LOPA only examines <u>one</u> scenario
- If there are more than one way to have a given loss event that would require multiple LOPA cases

LOPA Objective

- After a scenario has been identified the goal is to determine the actual Risk (order of magnitude resolution) with all of the safeguards that are in place
- Determine if additional safeguards are needed
- Determine the reliability that the new safeguard will require

LOPA

- Scenario Cause and Consequence pair is identified prior to LOPA
- The frequency of the Initiating Event (cause) needs to be determined (covered in last lecture)
- The frequency of the Loss Event (consequence) can be reduced by factoring in necessary Enabling Conditions
- The frequency of the Loss Event (consequence) can be reduced by factoring in appropriate Conditional Modifiers
- Identify the Independent Layers of Protection
  - Determine the probability that they will be successful
  - Determine if the Risk Tolerance for the Consequence has been achieved
  - Add additional IPL if necessary

Enabling Conditions

- This is a condition which makes the loss event possible after the initating event
- This is a condition that is not a failure, error, or a protection layer
- Some examples:
  - The initiating event leads to the loss event only when the process is in a certain condition
    - At start up, for example
  - If the temperature of the material is below its Flashpoint, then a release will not lead to a VCE (Vapor Cloud Explosion)
- It will be expressed as a dimensionless probability
- Not used in every LOPA
- There needs to be relevant data and understanding to support the use of enabling conditions

Enabling Condition – Campaign Risk

- The consequence will only be realized if the process unit is using a particular raw material or catalyst or processing a particular formula
- The presence of this condition is independent of the rest of the event sequence
  - The likelihood of the initiating event and the failure of the safeguards is independent of the whether the enabling condition is present

Enabling Condition – Campaign Risk

- In this example only about 10% of the time are they running a formula where runaway reaction is possible
- The highlighted area shows that in order to use this enabling condition we need to be certain that we would recognize loss of cooling water soon after it happens during the "safe" periods
  - Otherwise we may fail during the 90% safe time and as soon as we enter the "vulnerable" period we will be in a failure mode leading to a low event
  - The assumption here is that a loss of cooling water is only dangerous during the 10% of the time that we are in the "vulnerable" condition – but, if we don't detect failure during the other 90% then that is not true.

Scenario: Cooling water failure results in runaway reaction with potential for reactor overpressure, leakage, rupture, injuries and fatalities. Agitation assumed. Also assumed: Loss of cooling water can be detected before the reactor begins the condition where runaway reaction is possible.

		Frequency	Probability
...			
Initiating event	Loss of cooling water (revealed failure)	0.1/yr	
Enabling condition	Probability that reactor is in a condition where runaway reaction can occur on loss of cooling (average of about five one-week campaigns per year on an annual basis)		0.1
Loss event frequency without IPLs		0.01/yr	
...			

Seasonal Risks

- If it is too cold out for materials to be above flashpoint then the hazard is eliminated
  - In Buffalo there is a large portion of the year where it may be below the flashpoint of a given chemical
  - In Phoenix that portion of the time will be different
  - You would use the portion of time that you are above the flashpoint as your probability factor
- Humidity plays a part in the likelihood of a static discharge
  - The percentage of time that the relative humidity is below a certain level might be claimed as a factor in a LOPA
  - If you are above that level 75% of the time, then you are vulnerable 25% of the time and a factor of 0.25 might be claimed

Conditional Modifiers

- When the Risk Criteria endpoint is based on impact terms (e.g. fatalities) rather than primary loss events (e.g. Loss of Containment)
- Expressed as a dimensionless probability
- Not used in every LOPA
- Conditional Modifiers are not based on engineered or planned safeguards
- Conditional Modifiers are not specific to the scenario being evaluated
- Used to get a more accurate estimate of the probability of a scenario reaching a given endpoint

Conditional Modifiers

- Three common Conditional Modifiers
  - Probability that an ignition source will find the release
    - Without ignition the release does not lead to fire or explosion
  - Probability that someone will be in the affected area at the time of the event
    - If no one is present then no one gets injured
  - Probability that a person in the affected area will suffer injury or fatality
    - Being present does not guarantee that one will be injured
      - Projectiles won't necessarily hit you

Conditional Modifiers

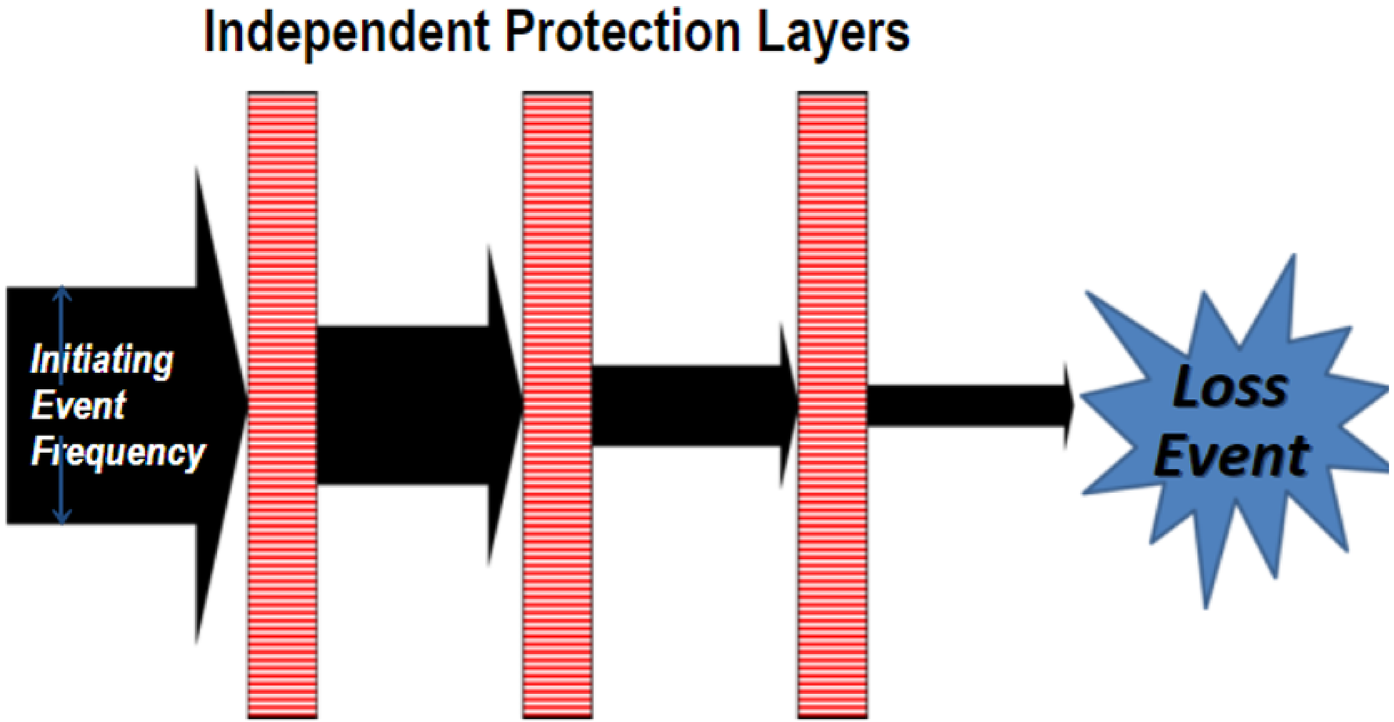
- Probability of Ignition
  - Is the release outside of an electrically classified area?
  - Does it cross a roadway?
  - Is there a continuous ignition source within range?
    - A flare or fired heater, etc
- Probability of Personnel Presence
  - Based on typical population of affected area
  - Consider whether the condition of the initiating event/scenario will draw operators to the area to respond (in which case Probability = 1)
  - Don't take double credit with time-at-risk enabling condition

Independent Protection Layers (IPL)

- A device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence
  - It must not be affected by the initiating event
  - It must work by itself, independently of any other protection layer
    - i.e. the failure of any other IPL must not affect its ability to stop the progression of events
- The effectiveness and independence of an IPL must be auditable
  - i.e. you have to be able to verify and document that it is working effectively

Independent Protection Layers

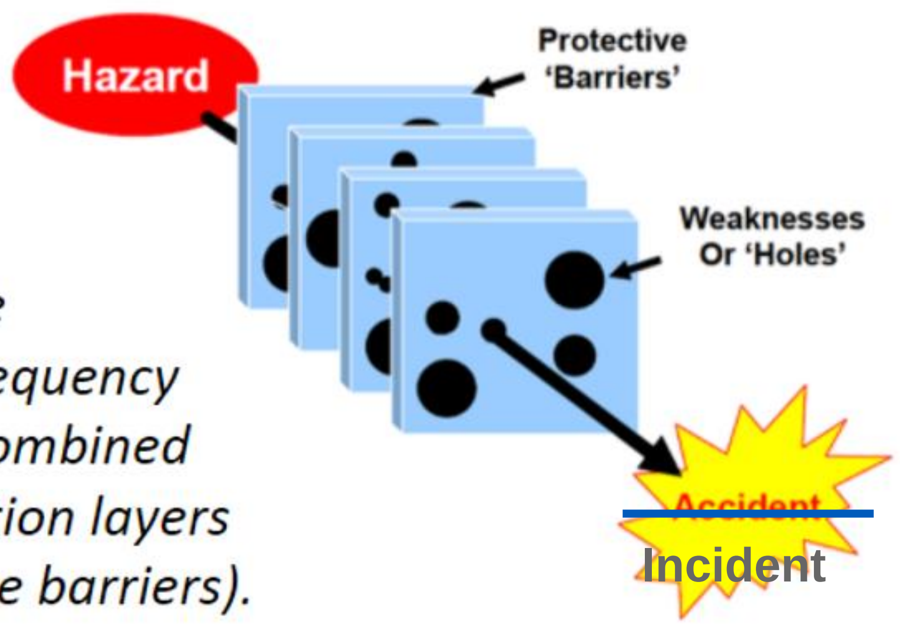
- Each IPL reduces the frequency of the Loss Event



Swiss Cheese Model

- Any “slice” can prevent the undesired event
- The “holes” in each layer all need to line up in order for the event to occur

Likelihood of a loss event is determined by the initiating event frequency (arrow) and the combined PFD of the protection layers (holes in protective barriers).



Examples of IPL

- BPCS (sometimes)
- Human Response Action
- Safety Instrumented Function (SIF), i.e. an “interlock”
- Emergency Relief System

Examples of Things that are NOT IPL

But are listed as “safeguards” in your HAZOP/FMEA/etc

- Operating Procedures and training
- Mechanical Integrity and Quality Assurance program
- Plant Emergency Response program
- Community Emergency Response programs