Process Hazards Analysis and Layer of Protection Analysis Core

PHA Definitions and Concepts

Learning Objectives

By the end of this lesson, you will be able to:

✓ Define PHA-related terms
✓ Describe the purpose and basic premise of a PHA
✓ Discuss the scope of a PHA
✓ Outline typical PHA outputs
✓ Describe PHA team make-up
## In This Section

### Definitions
- Design Envelope
- PHA Revalidation
- Process Hazard Analysis
- Hazard Evaluation

### Purpose
- What is Process Hazards Analysis used for?
- Basic premise
- Scope and Outputs

### Exercise – Death in the Oilfield

### Teams
- Full-time members
- Part-time members
- Roles

© PetroSkills, LLC. All rights reserved.
Definitions of Terms

**Design Envelope**
The intended limitations of the parameters of a process, including its associated equipment, inputs, and outputs

**Keep in Mind:**
When modifying a facility, consider process safety implications and take appropriate precautions

---

Definitions of Terms

**Process Hazards Analysis (PHA)/Hazard Evaluation (HE)**
- An organized effort to identify and analyze the significance of hazardous situations associated with a process or activity

**Keep in Mind:**
“PHA” is the domestic USA term for the activity known internationally as “Hazard Evaluation”. In this lesson, where the term PHA is used, it means both.

**PHA Revalidation**
- Not a PHA technique in itself
- An update and reconfirmation or modification of an existing PHA
- Triggers consist of six factors
Incidents Predictable by HAZOP

Recall the Duguid database in which he studied 562 process safety incidents and broke down the results into several tables. The table below, which resulted from that study, considers predictability of incidents using HAZOP. Duguid found that a little under half could have been predicted with a good HAZOP.

<table>
<thead>
<tr>
<th>Decade</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1950’s</td>
<td>11</td>
</tr>
<tr>
<td>1960’s</td>
<td>29</td>
</tr>
<tr>
<td>1970’s</td>
<td>125</td>
</tr>
<tr>
<td>1980’s</td>
<td>51</td>
</tr>
<tr>
<td>1990’s</td>
<td>33</td>
</tr>
</tbody>
</table>

**Total: 249 incidents (44.3%)**

Low numbers early on are understandable given the much smaller size of the industry, and low numbers more recently may be due to the very common use of PHA and other risk management techniques.
PHA Purpose

The purpose of a PHA is to find weaknesses in the design, or in the as-built facility; specifically, those weaknesses which have process safety implications.

**PHA Team**

<table>
<thead>
<tr>
<th>Will</th>
<th>Will Not</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make risk-based recommendations to eliminate the weaknesses or mitigate their risks</td>
<td>Perform the engineering to make necessary corrections</td>
</tr>
</tbody>
</table>

Some recommendations may involve further study, and scenarios which require more than a qualitative analysis may be passed on to a semi-quantitative analysis, usually Layer of Protection Analysis (LOPA).
**PHA Scope**

A PHA is **not** a design review, but will review design elements
- Assumes that the process design is final in order for it to accomplish its purpose and basic premise

Usually done at the end of the Front End Engineering Design (FEED)

Responsibility for resolutions must be outside scope of PHA

**Process Hazards Analysis Outputs**

PHA Analysis pinpoints weaknesses that affect:
- Employees
- Assets
- Business Opportunities
- Reputation
- Local Community
- Environment

Recommendations
- Risk-ranked
- Some actionable
- Others will require further review

PHA and LOPA
- LOPA added on to PHA to leverage multi-discipline team’s time and effort
Typical PHA Multi-Discipline Team

**Full-Time Members**
- Trained and experienced facilitator
- Scribe
- Qualified and experienced operator(s)
- Engineer(s)
  - Process
  - Mechanical
  - Facilities
  - Etc.

**Part-Time Members**
- Inspection
- Specialists
  - Fire protection
  - Metallurgist
  - Etc.
- Maintenance
- Vendor
- Safety
Learning Objectives

You are now able to:

☑ Define PHA-related terms
☑ Describe the purpose and basic premise of a PHA
☑ Discuss the scope of a PHAs
☑ Outline typical PHA outputs
☑ Describe PHA team make-up
Process Hazards Analysis and Layer of Protection Analysis Core

HAZOP and API 14C Methodologies

Learning Objectives

By the end of this lesson, you will be able to:

- Identify available PHA techniques and describe when they can be applied
- Explain the main elements of the HAZOP methodology
- Discuss the basis, method, and areas of application for API 14C
# In This Section

## Available PHA Techniques
- List
- Useful applications
- Commonly used

## HAZOP Methodology
- Flow chart
- Node example
- Worksheet
- Risk Ranking
- Limitations

## API 14C
- Overview
- Safety Analysis Examples
- Procedure
- API and HAZOP
Available PHA Techniques

- Human Reliability Analysis
- HAZOP
- What if/ Checklist
- Cause and Consequence Analysis
- Safety Review
- Event Tree Analysis
- Checklist Analysis
- Relative Ranking
- Fault Tree Analysis
- HAZID
- FMEA
- What-If Analysis
- Preliminary Hazards Analysis
- Event Tree Analysis

© PetroSkills, LLC. All rights reserved.
HAZOP Methodology

- Define “nodes” on P&IDs
- Define “normal” Flow, T, P, composition, etc.
- e.g. Flow, level, temperature, pressure
- e.g. none, more, less, reverse
- e.g. overpressure and rupture of piping
- e.g. control valve fails open

Select a process section or operating step

- Explain design intention of the process section or operating step
- Select a process variable or task
- Apply guide word to process variable or task to develop meaningful deviation
- Examine consequences associated with deviation (assuming all protection fails)
- List possible causes of deviation

Identify existing safeguards to prevent deviation

Repeat for all process sections or operating steps

- Repeat for all process variables or tasks
- Repeat for all guide words

Develop action items

Assess acceptability of risk based on consequences, causes, and protection

Safeguards adequate or inadequate?

e.g. Install larger relief valve orifice, reduce trim size in control valve

e.g. almonds, relief valve, etc.

HAZOP Node Example

Node 1

© PetroSkills, LLC. All rights reserved.
### Example HAZOP Worksheet

<table>
<thead>
<tr>
<th>Scenario Number</th>
<th>Deviation</th>
<th>Cause</th>
<th>Potential Consequences</th>
<th>Existing Safeguards</th>
<th>SR</th>
<th>L</th>
<th>R</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>No Flow</td>
<td>P-11A suction valve closed</td>
<td>Loss of production to degassing tower and downstream treating equipment</td>
<td>Manually operated gate valves have no history of closing on their own</td>
<td>3</td>
<td>0</td>
<td>3D</td>
<td>None</td>
</tr>
<tr>
<td>1-2</td>
<td>No Flow</td>
<td>P-11A suction valve closed</td>
<td>Pump cavitation and internal damage</td>
<td>Operator training on valve operation</td>
<td>2</td>
<td>2</td>
<td>2E</td>
<td>None</td>
</tr>
<tr>
<td>1-3</td>
<td>No Flow</td>
<td>Any valve between P-11A, C and C-1 closed</td>
<td>Increased pressure on gathering manifold with potential for relief valve opening to flare</td>
<td>Security fencing limiting public access</td>
<td>3</td>
<td>2</td>
<td>2C</td>
<td>None</td>
</tr>
<tr>
<td>1-4</td>
<td>No Flow</td>
<td>Line between gathering manifold and C-1 plugged</td>
<td>Environmental excursion at flare</td>
<td>Pump design tolerates short term cavitation</td>
<td>2</td>
<td>2</td>
<td>2E</td>
<td>None</td>
</tr>
<tr>
<td>1-5</td>
<td>No Flow</td>
<td></td>
<td>Public alarm</td>
<td>PSI rated for full shutoff pressure</td>
<td>3</td>
<td>3</td>
<td>3A</td>
<td>None</td>
</tr>
<tr>
<td>1-6</td>
<td>No Flow</td>
<td></td>
<td>Negative publicity</td>
<td>Flare equipped with auxiliary steam to minimize smoking</td>
<td>2</td>
<td>2</td>
<td>2E</td>
<td>None</td>
</tr>
</tbody>
</table>

**Note:**
1. SR = Severity of Consequence without safeguards
2. L = Likelihood of Consequence occurring with functional safeguards
3. R = Risk as determined from a risk matrix

---

### Risk Ranking Matrix

<table>
<thead>
<tr>
<th>Frequency of Occurrence</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Frequent</td>
<td>1A</td>
</tr>
<tr>
<td>(B) Probable</td>
<td>2A</td>
</tr>
<tr>
<td>(C) Occasional</td>
<td>3A</td>
</tr>
<tr>
<td>(D) Remote</td>
<td>1E</td>
</tr>
</tbody>
</table>

**Risk Categories:**
- High
- Serious
- Medium
- Low

---

© PetroSkills, LLC. All rights reserved.
HAZOP Limitations

1. Something not on the P&ID
2. Operating procedure failure
3. Straight mechanical failure
4. Combination of possible events
5. Events that are not related to a guide word
API 14C Practice

- Recommended practice for offshore production platforms
- Use has extended beyond offshore

What is it?

- Analyzes different equipment types as independent units assuming worst case “undesirable events” applicable to that equipment type.
  - Causes
  - Effects and detectable abnormal conditions
  - Protection methods
- Defines the circumstances under which a safeguard may be deleted

API 14C Premise

If protection is provided for each equipment component on a standalone basis, a system of components will also be protected, regardless of configuration.

Specific configuration of process equipment is not considered.
Safety Analysis Examples

Safety Analysis Tables (SAT)

Safety Analysis Tables (SATs) are available for all commonly used types of process equipment, and they identify the undesirable events, the possible causes, and the means of detection for each one. The defined guidewords suggest a similarity to the HAZOP method at this point, except that the potential causes are already defined.

<table>
<thead>
<tr>
<th>Undesirable Event</th>
<th>Cause</th>
<th>Detectable Abnormal Condition at Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overpressure (suction)</td>
<td>Excess inflow</td>
<td>High pressure</td>
</tr>
<tr>
<td></td>
<td>Failure of suction pressure control system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compressor or driver malfunction</td>
<td></td>
</tr>
<tr>
<td>Overpressure (discharge)</td>
<td>Blocked or restricted discharge line</td>
<td>High pressure</td>
</tr>
<tr>
<td></td>
<td>Excess back pressure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High inlet pressure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Overspeed</td>
<td></td>
</tr>
<tr>
<td>Leak</td>
<td>Deterioration</td>
<td>Low pressure</td>
</tr>
<tr>
<td></td>
<td>Erosion</td>
<td>High gas concentration (building)</td>
</tr>
<tr>
<td></td>
<td>Corrosion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Impact damage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vibration</td>
<td></td>
</tr>
<tr>
<td>Excess Temperature</td>
<td>Compressor valve failure</td>
<td>High temperature</td>
</tr>
<tr>
<td></td>
<td>Cooler failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Excess compression ratio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Insufficient flow</td>
<td></td>
</tr>
</tbody>
</table>
Safety Analysis Checklist (SAC)

The Safety Analysis Checklist (SAC) identifies the required safeguards, and the acceptable reasons for not installing them. For example, item “f” requires a relief valve on the discharge of the compressor, unless there is a non-isolatable relief valve downstream of the compressor and upstream of any cooler, or the compressor is kinetic (usually centrifugal) and is incapable of developing pressure greater than the maximum allowable working pressure of the downstream piping or the compressor itself. Rather than have the team decide whether safeguards are adequate, API 14C defines the safeguards and requires that they be provided unless one of the allowable exceptions is met. It is a prescriptive method, which provides consistency and saves time. It does not allow for risk-based decision making.

Safety Analysis Checklist (SAC) – Compressors

a) High Pressure Sensor (PSH)—suction.
   1. PSH installed.
   2. Each input source is protected by a PSH that will also protect the compressor.

b) High Pressure Sensor (PSH)—discharge.
   1. PSH installed.
   2. Compressor is protected by a downstream PSH, located upstream of any cooler, that cannot be isolated from the compressor.

c) Low Pressure Sensor (PSL)—suction.
   1. PSL installed.
   2. Each input source is protected by a PSL that will also protect the compressor.

d) Low Pressure Sensor (PSL)—discharge.
   1. PSL installed.
   2. Compressor is protected by a downstream PSL that cannot be isolated from the compressor.

e) Pressure Safety Valve (PSV)—suction.
   1. PSV installed.
   2. Compressor is protected by a downstream PSL that cannot be isolated from the compressor.

f) Pressure Safety Valve (PSV)—discharge.
   1. PSV installed.
   2. Compressor is protected by a downstream PSV, located upstream of any cooler, that cannot be isolated from the compressor.
   3. Compressor is kinetic energy type and incapable of generating a pressure greater than the maximum allowable working pressure of the compressor or discharge piping.

gh) Check Valve (FSV)—final discharge.
   1. FSV installed.

h) High Temperature Sensor (TSH).
   1. TSH installed.
Safety Analysis Functional Evaluation (SAFE)

The Safety Analysis Functional Evaluation (SAFE) chart consolidates the protections into a form, which is a modified FMEA. For each piece of equipment, including major piping such as the incoming and outgoing pipelines, the SAFE chart shows each safeguard and the SAC reference number if that safeguard is not installed. Shutdown devices and their functions are identified. It is possible to quickly see how any system or subsystem is protected, and whether or not the requirements of API 14C have been met.
API 14C Procedure

1. Describe the process using a P&ID or detailed flow schematic and establish operating parameters.

2. From the Safety Analysis Tables (SATs), verify the need for basic safety devices for each process component as an individual unit. Use the Safety Analysis Checklists (SACs) for the individual components to justify the elimination of safety devices when each process.

3. Develop SAT/SAC tables for any process components not covered in the RP.

4. Use the Safety Analysis Function Evaluation (SAFE) chart to integrate all safety devices and self-protected equipment into a complete safety system.

5. For new systems, add the safety devices to the P&ID’s.

6. For existing systems, compare the SAFE chart with the existing safety system and make modifications as required.
## API 14C Benefits

<table>
<thead>
<tr>
<th>Simple</th>
<th>API 14C has been adopted as ISO 10418</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistent</td>
<td>ISO 10418 also allows for the use of risk-based methods</td>
</tr>
<tr>
<td>Removes subjectivity associated with incident frequency/severity estimation</td>
<td>Originated from API RP 14C 4th edition in 1993</td>
</tr>
<tr>
<td>Less time and manpower</td>
<td>Current (2nd edition) issued in 2003</td>
</tr>
<tr>
<td>Prescriptive, not “risk-based”</td>
<td></td>
</tr>
<tr>
<td>More appropriate for less complex facilities</td>
<td></td>
</tr>
</tbody>
</table>

© PetroSkills, LLC. All rights reserved.
Learning Objectives

You are now able to:

✓ Identify available PHA techniques and describe when they can be applied
✓ Explain the main elements of the HAZOP methodology
✓ Discuss the basis, method, and areas of application for API 14C
Learning Objectives

By the end of this lesson, you will be able to:

- Compare the different PHA techniques available
- Describe a PHA revalidation
- Recognize the six factors that may trigger a PHA revalidation
- Identify when different PHA techniques can be used during the process lifecycle
### In This Section

#### Comparison of PHA Techniques
- Advantages
- Disadvantages
- Common applications

#### PHA Revalidation
- Description
- Six triggers

#### PHA Technique Timing
- At what stages of a facility life cycle is each technique likely to be used?
# Most Commonly Used Techniques Comparison

<table>
<thead>
<tr>
<th>Technique</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Primary Application(s)</th>
<th>Project Phase(s)</th>
</tr>
</thead>
</table>
| **HAZOP Analysis** | Pinpoints weaknesses in the design and operation of facilities that could lead to unintended releases, fires or explosions with impacts to employees, assets, business opportunities, the local community and environment  
Makes risk-based recommendations to eliminate the weaknesses or mitigate their risk  
Is the most thorough and systematic PHA technique | Typically takes more resources and time  
Not as easy to focus on a hazard or change because it looks more at systems/processes | New capital projects or major modifications to existing processes  
On-going operations | End of detailed design when design is final  
Any time during the normal operating life of the process |
| **What-If / Checklist Analysis (W-I/CL)** | Combines creative team brainstorming of the What-if technique with the systematic features of the Checklist analysis  
Focuses easily on area(s) of concern and changes  
Is most often used in conjunction with management of change | Less systematic than the HAZOP technique  
More reliant on team member expertise and checklist quality to produce quality results | Capital projects/process modifications/Management of change  
Less complex systems  
PHA Revalidation | Process development  
Operations, Maintenance, Modification |
Safety Analysis Examples

Safety Analysis Tables (SAT)

Safety Analysis Tables (SATs) are available for all commonly used types of process equipment, and they identify the undesirable events, the possible causes, and the means of detection for each one. The defined guidewords suggest a similarity to the HAZOP method at this point, except that the potential causes are already defined.

<table>
<thead>
<tr>
<th>Undesirable Event</th>
<th>Cause</th>
<th>Detectable Abnormal Condition at Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overpressure (suction)</td>
<td>Excess inflow</td>
<td>High pressure</td>
</tr>
<tr>
<td></td>
<td>Failure of suction pressure control system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compressor or driver malfunction</td>
<td></td>
</tr>
<tr>
<td>Overpressure (discharge)</td>
<td>Blocked or restricted discharge line</td>
<td>High pressure</td>
</tr>
<tr>
<td></td>
<td>Excess back pressure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High inlet pressure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Overspeed</td>
<td></td>
</tr>
<tr>
<td>Leak</td>
<td>Deterioration</td>
<td>Low pressure</td>
</tr>
<tr>
<td></td>
<td>Erosion</td>
<td>High gas concentration (building)</td>
</tr>
<tr>
<td></td>
<td>Corrosion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Impact damage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High inlet pressure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Overspeed</td>
<td></td>
</tr>
<tr>
<td>Excess Temperature</td>
<td>Compressor valve failure</td>
<td>High temperature</td>
</tr>
<tr>
<td></td>
<td>Cooler failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Excess compression ratio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Insufficient flow</td>
<td></td>
</tr>
</tbody>
</table>
Safety Analysis Checklist (SAC)

The Safety Analysis Checklist (SAC) identifies the required safeguards, and the acceptable reasons for not installing them. For example, item “f” requires a relief valve on the discharge of the compressor, unless there is a non-isolatable relief valve downstream of the compressor and upstream of any cooler, or the compressor is kinetic (usually centrifugal) and is incapable of developing pressure greater than the maximum allowable working pressure of the downstream piping or the compressor itself. Rather than have the team decide whether safeguards are adequate, API 14C defines the safeguards and requires that they be provided unless one of the allowable exceptions is met. It is a prescriptive method, which provides consistency and saves time. It does not allow for risk-based decision making.

Safety Analysis Checklist (SAC) – Compressors

a) High Pressure Sensor (PSH)—suction.
   1. PSH installed.
   2. Each input source is protected by a PSH that will also protect the compressor.

b) High Pressure Sensor (PSH)—discharge.
   1. PSH installed.
   2. Compressor is protected by a downstream PSH, located upstream of any cooler, that cannot be isolated from the compressor.

c) Low Pressure Sensor (PSL)—suction.
   1. PSL installed.
   2. Each input source is protected by a PSL that will also protect the compressor.

d) Low Pressure Sensor (PSL)—discharge.
   1. PSL installed.
   2. Compressor is protected by a downstream PSL that cannot be isolated from the compressor.

e) Pressure Safety Valve (PSV)—suction.
   1. PSV installed.
   2. Compressor is protected by a downstream PSL that cannot be isolated from the compressor.

f) Pressure Safety Valve (PSV)—discharge.
   1. PSV installed.
   2. Compressor is protected by a downstream PSV, located upstream of any cooler, that cannot be isolated from the compressor.
   3. Compressor is kinetic energy type and incapable of generating a pressure greater than the maximum allowable working pressure of the compressor or discharge piping.

g) Check Valve (FSV)—final discharge.
   1. FSV installed.

h) High Temperature Sensor (TSH).
   1. TSH installed.
Safety Analysis Functional Evaluation (SAFE)

The Safety Analysis Functional Evaluation (SAFE) chart consolidates the protections into a form, which is a modified FMEA. For each piece of equipment, including major piping such as the incoming and outgoing pipelines, the SAFE chart shows each safeguard and the SAC reference number if that safeguard is not installed. Shutdown devices and their functions are identified. It is possible to quickly see how any system or subsystem is protected, and whether or not the requirements of API 14C have been met.
### Other Techniques

<table>
<thead>
<tr>
<th>Technique</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Primary Application(s)</th>
<th>Project Phase(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Review</td>
<td>Ensures plant and its operating and maintenance practices match design intent and construction standards</td>
<td>Less structured Quality dependent on team expertise</td>
<td>Capital projects Management of change Broad brush look at inherent hazards of a large plant, complex process or design aspect</td>
<td>Research, Process Development</td>
</tr>
<tr>
<td>Checklist Analysis</td>
<td>Used primarily to ensure that organizations are complying with standard practices</td>
<td>Limited by author’s experience Less structured Quality dependent on team expertise</td>
<td>Capital projects Broad brush look at inherent hazards of a large plant, complex process or design aspect</td>
<td>Research, Process Development</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Confirm “cookie cutter” facility meets master design (e.g., well head facility)</td>
<td></td>
<td>Detail Design and Construction</td>
</tr>
</tbody>
</table>

### Other Techniques

<table>
<thead>
<tr>
<th>Technique</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Primary Application(s)</th>
<th>Project Phase(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminary Hazards Analysis</td>
<td>Evaluates hazards early in the life of a process</td>
<td>Intended to highlight and prioritize hazards and areas of concern for further treatment during Detail Design and Construction phase</td>
<td>Capital projects Management of change</td>
<td>Research, Process Development</td>
</tr>
<tr>
<td>What-If Analysis</td>
<td>Identifies hazards, hazardous situations, specific accident events and concerns that could produce undesirable consequences</td>
<td>Relies entirely on expertise of team and their ability to brainstorm Can be very effective when combined with the Checklist technique as in the What-If/Checklist Technique</td>
<td>Capital Projects Management of change Useful whenever there is a need to focus quickly on a change or hazard</td>
<td>All/Any</td>
</tr>
</tbody>
</table>
API 14C Procedure

1. Describe the process using a P&ID or detailed flow schematic and establish operating parameters.

2. From the Safety Analysis Tables (SATs), verify the need for basic safety devices for each process component as an individual unit. Use the Safety Analysis Checklists (SACs) for the individual components to justify the elimination of safety devices when each process.

3. Develop SAT/SAC tables for any process components not covered in the RP.

4. Use the Safety Analysis Function Evaluation (SAFE) chart to integrate all safety devices and self-protected equipment into a complete safety system.

5. For new systems, add the safety devices to the P&ID’s.

6. For existing systems, compare the SAFE chart with the existing safety system and make modifications as required.
<table>
<thead>
<tr>
<th>Technique</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Primary Application(s)</th>
<th>Project Phase(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Reliability Analysis</td>
<td>Identifies potential human error and their effects, or is used to identify the underlying causes of human errors</td>
<td>Focus is only on human part of the human-machine interface</td>
<td>To evaluate previously identified potential human error scenarios</td>
<td>Any/All</td>
</tr>
<tr>
<td>Failure Modes and Effects Analysis (FMEA)</td>
<td>Identifies single equipment and system failure modes and each failure mode’s potential effect(s) on the system or process</td>
<td>Outputs are more of a preventive maintenance schedule, than a hazards analysis</td>
<td>Equipment reliability</td>
<td>Operations, Maintenance and Modification</td>
</tr>
<tr>
<td></td>
<td>Most often used for preventing and/or resolving equipment reliability issues</td>
<td>Not actually used by many companies as a PHA technique</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**PHA Revalidation**

### Description

- Not a stand-alone PHA technique
- Not valid indefinitely
- Review and revalidate PHAs every several years
- Is a regulatory requirement in the USA every five years
- Where not required by regulation, it is a good engineering practice to apply it every 3-10 years

### Changes in process or equipment

- Gaps or deficiencies in prior PHA
- Incident history
- New knowledge about the operation
- Unresolved previous PHA recommendations
- Updated or changed regulatory or company requirements
In terms of timing, look at the process lifecycle and see which techniques are most commonly used at which stages.

A **safety review** may be done at a wide range of points. It is sometimes done very early on, and may also be done during construction and startup. Safety may then be revisited during normal operations, expansion, and modification, and again at decommissioning.

**Checklist** will be used at almost any point, other than R&D or incident investigation. This includes the stages of conceptual design, pilot plan, detailed design, construction, startup, operation, modification, and decommissioning.

**Relative ranking** is used often in R&D and conceptual design, but may also be used in the early stages of designing, expansion, or modification.

**Preliminary hazards analysis** is performed through all the preliminary stages, including the design phase, but is generally not used during routine operation or an incident investigation. However, it may be used at any other point.

**What-if** is used across the board, throughout the lifecycle. This may be the creative brainstorming what-if technique. A combination of what-if and checklist is used at all design stages, routine operation, and modification.

**HAZOP** is used during design, pilot plan, feed, detailed engineering, routine operations, changes, modifications, and sometimes also in incident investigation.

**FMEA** could be applied at the same stages as a HAZOP, fault tree, event tree, and as cause consequence analysis.

**Human reliability analysis** would not normally be done during R&D, conceptual design, or during commissioning, but could be used at every stage in between them.
Learning Objectives

You are now able to:

✓ Compare the different PHA techniques available
✓ Describe a PHA revalidation
✓ Recognize the six factors that may trigger a PHA revalidation
✓ Identify when different PHA techniques can be used during the process lifecycle
Learning Objectives

By the end of this lesson, you will be able to:

✔ Define Layer of Protection Analysis
✔ Describe the purpose of Layer of Protection Analysis
✔ Discuss Layers of Protection, Onion Skin, and Swiss Cheese models
In This Section

Layer of Protection Analysis
- Definition
- Purpose

Typical Layers of Protection
- Layers of Protection
- Onion Skin Model
- Swiss Cheese Model
**What is Layer of Protection Analysis?**

A semi-quantitative risk assessment technique

Evaluates risks by orders of magnitude

Selected accident scenarios

Builds on the information developed in qualitative hazard evaluation

---

**Layers of Protection**

Mitigate

Passive Protection Layer

Active Protection Layer

Emergency Response Layer

Prevent

Safety Layer

Emergency Shutdown

Process Shutdown

Operator Intervention

Basic Process Control System

© PetroSkills, LLC. All rights reserved.
**Onionskin Diagram**

Hazard are contained by multiple protective barriers
- Barriers may have weaknesses, or “holes”
- When holes align, hazard, energy, or chemical, is released, resulting in the potential for harm
- Barriers may be physical engineered containment or behavioral controls dependent on people
- Holes can be latent/incipient, or actively opened by people

**Swiss Cheese Model**

- Community Emergency Response
- Plant Emergency Response
- Physical Protection (Relief Devices and Dikes)
- Automatic Action SIS or ESD
- Critical Alarms and Operator Intervention
- Process Alarms and Operator Supervision
- Plant Design

Accident

Hazard

Protective ‘Barriers’

Weaknesses or ‘Holes’
Learning Objectives

You are now able to:

✓ Define Layer of Protection Analysis
✓ Describe the purpose of Layer of Protection Analysis
✓ Discuss Layers of Protection, Onion Skin, and Swiss Cheese models
# Process Hazards Analysis and Layer of Protection Analysis Core

## LOPA Procedure

**Learning Objectives**

By the end of this lesson, you will be able to:

- Discuss the relationship between HAZOP and LOPA
- List and describe the steps in a LOPA procedure
- List the criteria for choosing independent protection layers (IPLs)
- Define conditional modifiers
- Discuss Safety Integrity Levels and their relationship with Safety Instrumented Functions
# Process Hazards Analysis and Layer of Protection Analysis Core

## In This Section

<table>
<thead>
<tr>
<th>Overview of LOPA</th>
<th>LOPA Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Relationship between HAZOP and LOPA</td>
<td>• Steps in the procedure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Independent Protection Layers and Conditional Modifiers</th>
<th>LOPA Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Definitions</td>
<td>• Simple example</td>
</tr>
<tr>
<td>• Criteria</td>
<td>• Calculation</td>
</tr>
</tbody>
</table>

© PetroSkills, LLC. All rights reserved. 40
Relationship Between HAZOP and LOPA

Any LOPA scenario includes an initiating event and an impact event. Possible causes in a HAZOP maps directly to initiating cause in LOPA, and consequences maps to impact event description. Severity and likelihood will feed the impact event severity level and initiating cause frequency, though some evaluation may be needed. That is not necessarily a direct map. Safeguards and actions required will contribute to the protection layers section, while actions required will also contribute to the SIF integrity level.
LOPA Procedure

1. Define and document risk acceptance criteria
2. Define the consequence and severity of the impact event
3. Identify initiating events and their associated frequencies
   Usually taken from the PHA study results
4. Select initiating event – impact event pair
5. Identify IPL’s and their associated PFD’s

6. Define any appropriate frequency modifiers
   - Probability of ignition
   - Probability of personnel in area
   - Etc.

7. Calculate intermediate event likelihood
   Compare to risk acceptance criteria

8. If risk acceptance criteria is not satisfied…
   Determine what Safety Instrumented Functions (SIF) are needed and the Safety Integrity Levels (SIL) required

9. If SIL > 2, consider QRA or change to process
Independent Protection Layers

**IPL is a device, system or action that is:**
- Capable of preventing a scenario from proceeding to its undesired consequence
- Independent of the initiating event or the action of any other layer of protection associated with the scenario

**Effective in preventing the consequence when it functions as designed**

**Independent of the initiating event and the components of any other IPL already claimed for the same scenario**

**Auditable:** the assumed effectiveness must be capable of validation (by documentation, review, testing, etc.)

Conditional Modifiers

**What are conditional modifiers?**
- Other factors which are neither failures nor protection layers
  - Probability of ignition
  - Probability that personnel are in the affected area
  - Probability of fatal injury given exposure

*Conditional modifiers affect calculated risk. Use with discretion.*
## General Format of LOPA Table

<table>
<thead>
<tr>
<th>Element Number</th>
<th>Equipment/Function</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### LOPA Example

Select Pause on your video player and read the example below.

A vessel is used to store high vapor pressure condensate. The level in the vessel is controlled by a level controller which operates a control valve on the tank inlet. If the vessel is overfilled, condensate would be released thru a PSV and be contained in a dike though some vapor would form. A HAZOP indicated the LIC might fail, overfilling the tank. If the dike fails, some liquid and/or vapor would escape from the dike. The presence of an ignition source near the tank is possible from time to time and personnel are in the area occasionally, which could result in a fatality.

The operating company wants to determine if the existing facility satisfies their corporate risk criteria, or if any changes are required and if so how extensive they would need to be.
From the worksheet, the probability of fire is:

\[0.1 \times 0.01 \times 1 = 1 \times 10^{-3}\]

\[P(\text{BPCS loop failure}) \times P(\text{dike failure}) \times P(\text{ignition})\]

The corporate risk target for fire is not being met by a factor of:

\[\frac{1 \times 10^{-3}}{1 \times 10^{-4}} = 10\]

The probability of a fatality is \(2.5 \times 10^{-4}\) which exceeds the corporate risk target by a factor of:

\[\frac{2.5 \times 10^{-4}}{1 \times 10^{-5}} = 25\]

Conclusion: the current design doesn’t meet either corporate risk target.

**Possible solution**

- Install a separate high-level shutdown function
  - Need a Safety Instrumented Function (SIF) with a Safety Integrity Level (SIL) = 1 that achieves a Risk Reduction Factor (RRF) of at least 25.
- What would this look like?
  - Will be discussed in more detail in the Safety Instrumented Systems section
### Safety Integrity Levels

<table>
<thead>
<tr>
<th>SIL</th>
<th>PFD Range</th>
<th>Safety Availability (1-PFD)</th>
<th>Risk Reduction Factor (1/PFD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$10^{-1} \rightarrow 10^{-2}$</td>
<td>90 – 99%</td>
<td>10 – 100</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-2} \rightarrow 10^{-3}$</td>
<td>99 – 99.9%</td>
<td>100 – 1,000</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-3} \rightarrow 10^{-4}$</td>
<td>99.9% - 99.99%</td>
<td>1,000 – 10,000</td>
</tr>
<tr>
<td>4</td>
<td>$10^{-4} \rightarrow 10^{-5}$</td>
<td>&gt; 99.99%</td>
<td>10,000 – 100,000</td>
</tr>
</tbody>
</table>

The SIL is associated with a specific SIF
- *not* the entire SIS
- *not* an individual component of the SIF,
  - *e.g.* sensor, final element
Learning Objectives

You are now able to:

✓ Discuss the relationship between HAZOP and LOPA
✓ List and describe the steps in a LOPA procedure
✓ List the criteria for choosing independent protection layers (IPLs)
✓ Define conditional modifiers
✓ Discuss Safety Integrity Levels and their relationship with Safety Instrumented Functions
PetroAcademy™ Process Safety Engineering Skill Modules

- Process Safety Risk Analysis and Inherently Safer Design Core
- Process Hazards Analysis and Layers of Protection Analysis Core
  - Leakage and Dispersion of Hydrocarbons Core
  - Combustion Behavior of Hydrocarbons Core
  - Sources of Ignition and Hazardous Area Classification Core
  - Specific Plant Systems and Equipment Core
  - Relief and Flare Systems Core
  - Historical Incident Databases, Plant Layout and Equipment Spacing Core
  - SIS, Monitoring and Control Core
  - Fire Protection Systems Core