LOPA
An efficient Safety Barrier Management tool
Layer of protection according to IEC-61511

COMMUNITY EMERGENCY RESPONSE
  Emergency broadcasting

PLANT EMERGENCY RESPONSE
  Evacuation procedures

MITIGATION
  Mechanical mitigation system
  Safety Instrumented control system
  Safety instrumented mitigation systems
  Operator supervision

PREVENTION
  Mechanical protection system
  Process alarms with operator corrective action
  Safety Instrumented control system
  Safety instrumented prevention systems

CONTROL and MONITORING
  Basic Process Control Systems
  Monitoring system (process alarms)
  Operator supervision

PROCESS
What are we protecting?

COMMUNITY EMERGENCY RESPONSE
- Emergency broadcasting

PLANT EMERGENCY RESPONSE
- Emergency Power
- Emergency Communication
- Emergency Lighting

MITIGATION (Fire & Explosion) = PREVENTION OF ESCALATION
- Fire & Gas Detection System
- Emergency Shutdown (ESD-1)
- Blowdown & Drainage System
- Active & Passive Fire Protection

MITIGATION (Process Safeguarding)
- Mechanical mitigation system (e.g., pressure relief, dike, …)

PREVENTION
- Process Shutdown (ESD-3 & ESD-2)
- Process alarms with operator corrective action

CONTROL and MONITORING
- Basic Process Control Systems
- Monitoring system (process alarms)
- Operator supervision

PROCESS (EUC)

EUC: Equipment Under Control
AUC: Area Under Control
No Major Accident!

An occurrence resulting from **uncontrolled** developments in the course of the operation of any onshore establishment or pipeline or offshore installation, and leading to serious danger to human health or the environment, immediate or delayed, inside or outside the onshore establishment or offshore installation, and involving one or more **dangerous substances**.

This includes in particular a major:
- Emission
- Fire
- Explosion.
**Major Accident Hazard Tree**

*From API 14J*

![Major Accident Hazard Tree Diagram]

- **Vessel Overflow**
  - Inflow exceeds outflow

- **Equipment Failure**
  - Overpressure*
  - Leak: Corrosion, Erosion, Maintenance
  - Excessive temperature*
  - Hit by object
  - Material; quality
  - Sudden failure of mechanical seal*

- **Opening a closed system**
  - Valve operation

- **Vent/flare system discharge**
  - Inadequate scrubber size
  - Scrubber inflow exceeds outflow*

- **Oil Spill**
  - Escaping gas
  - Inadequate drain system
  - Water pollution

- **Air Pollution**
  - Inadequate scrubber size

- **Injury**
  - Asphyxiation/poisoning
  - Burn

- **Fire**
  - Large fire
  - Asphyxiation/poisoning
  - Burns

- **Explosion**
  - Electric shock
  - Physical impact

- **Electric shock**
  - Lightning
  - Electrical short
  - Inadequate ground
  - Exposed live connections

- **Physical impact**
  - Fall
  - Tripping
  - Slip on slick surfaces
  - Hit by object
  - Overpressure
  - Cranes
  - Boats
  - Helicopter

- **Large fire**
  - Insufficient or inoperable fire fighting equipment
  - Wrong location of F/F equipment
  - Inability of shut off fuel
  - Lack of adequate warning

- **Asphyxiation/poisoning**
  - Gas leak in confined space
  - Leak of toxic chemicals
  - Discharge of fire extinguishing agent in confined space
  - Smoke from fire

*Sources which can be anticipated by sensing charges in process conditions*
Hierarchy of Safety Critical Barriers


Incident Prevention Post Incident Control and Mitigation Gas Release Escalating Consequence

Safe Operation
Life Cycle HSE Management
Example
HSE Management for PSV
Hierarchy of Safety Critical Barriers

- Inherently Safe
- Layout & Safety distances
- Structural integrity
- Process Containment
- Ignition Control
- Process Safeguarding
- F&G Detection Systems
- ESD/EDP Systems
- Emergency Response
- Lifesaving

Safe Operation

Incident Prevention

Post Incident Control and Mitigation

Gas Release

Escalating Consequence
Overpressure Safety Barriers

Design Quality Assurance

Safe Operating Pressure

Code Compliance
HAZOP
Process Control Strategy & Tuning
Operating Procedures

High Pressure Trip
Pressure Relief Valve

Multiple Failures

Gas Release

Incident Prevention

Post Incident Control and Mitigation

Overpressure

ADEPP Academy
PSV Safety Barriers

EPC Contractor
Quality Assurance

Client Quality Assurance

Overpressure < Failure pressure of vessel

Design
Procurement
Manufacturing
Construction
Commissioning
Maintenance

Vessel Failure

Incident Prevention

Post Incident Control and Mitigation

Pressure Relief Failure
There are no Perfect Safety Barriers

Probability of failure on demand can be reduced or eliminated by different techniques including:

- Intrinsically safe,
- Fail safe,
- Redundancy,
- Shorter inspection, test and planned maintenance routines and more,
- Advanced technology.
LOPA should be repeated for **ALL** undesirable deviation within equipment

<table>
<thead>
<tr>
<th>Undeirable event</th>
<th>No. of protection Layers</th>
<th>Protection Adequate?</th>
<th>Achieved SIL</th>
<th>Remarks/ Recommendations / Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overpressure (Suction)</td>
<td>0 1 2 3 4 5</td>
<td>3</td>
<td>Yes</td>
<td>4</td>
</tr>
<tr>
<td>Excluding fire</td>
<td></td>
<td></td>
<td></td>
<td>For parallel operation suction scrubber is inherently safe: - design pressure = 210 barg - Surge recycle line pressure = 144 barg</td>
</tr>
<tr>
<td>Overpressure (Discharge)</td>
<td>0 1 2 3 4 5</td>
<td>4</td>
<td>Yes</td>
<td>4</td>
</tr>
<tr>
<td>Excluding fire</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low pressure</td>
<td>0 1 2 3 4 5</td>
<td>3</td>
<td>Yes</td>
<td>1</td>
</tr>
<tr>
<td>Excess Temperature</td>
<td>0 1 2 3 4 5</td>
<td>3</td>
<td>Yes</td>
<td>1</td>
</tr>
<tr>
<td>Low Temperature</td>
<td>0 1 2 3 4 5</td>
<td>3</td>
<td>Yes</td>
<td>1</td>
</tr>
<tr>
<td>Liquid overflow in suction scrubber</td>
<td>0 1 2 3 4 5</td>
<td>2</td>
<td>Yes</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No considerable liquid is expected in this vessel.</td>
</tr>
<tr>
<td>Reverse flow</td>
<td>0 1 2 3 4 5</td>
<td>3</td>
<td>Yes</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Double check valve with two different type are considered as SIL2 secondary protection.</td>
</tr>
<tr>
<td>Leak</td>
<td>0 1 2 3 4 5</td>
<td>3</td>
<td>Yes</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1PZA-2p20-LL can be an indication of gas leak to atmosphere.</td>
</tr>
<tr>
<td>External fire</td>
<td>0 1 2 3 4 5</td>
<td>2</td>
<td>Yes</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The suction scrubbers and pipeworks outside compressor house are protected by the PFP.</td>
</tr>
</tbody>
</table>

L0- Inherently Safe, L1- BPCS, L2- Alarm, operator, L3- SIS, L4- Mechanical/ Relief devices
L5- Physical protection: L5.1 - ESD, L5.2 - EDP, L5.3 - Passive fire protection, L5.4 - Active fire protection
API 14C
A prescriptive approach to LOPA
Process Safeguarding

Following scenarios are the most common undesirable events which can lead to an Emission and/or Fire & Explosion Major Accident in a plant which processes the flammable and/or toxic materials:

• Overpressure
• Leak
• Liquid Overflow
• Gas Blowby
• Under-pressure
• Excess Temperature
• Direct Ignition Source
• Excess combustion vapour

According API 14C at least two levels of protection independent and diverse shall be provided wherever these hazards are credible.
Example: Overpressure Protection

**Primary Protection:** High Pressure Trip
**Function:** Stop inlet flow
**Type:** Instrumented Based

**Secondary Protection:** Pressure Relief Valve
**Function:** Discharge the excess materials to safe location
**Type:** Mechanical Based

Diagram:
- Inlet ESD Valve
- PSH
- To Flare
## Example of Safety Analysis Table for Compressor

<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&lt;br&gt;Failure of suction pressure&lt;br&gt;Control system&lt;br&gt;Compressor or driver malfunction</td>
<td>High Pressure</td>
</tr>
<tr>
<td>Overpressure (Discharge)</td>
<td>Blocked or restricted discharge line&lt;br&gt;Excess back pressure&lt;br&gt;High inlet pressure&lt;br&gt;Over-speed</td>
<td>High pressure</td>
</tr>
<tr>
<td>Leak</td>
<td>Deterioration&lt;br&gt;Erosion&lt;br&gt;Corrosion&lt;br&gt;Impact damage&lt;br&gt;Vibration</td>
<td>Low pressure&lt;br&gt;High Gas Concentration (Building)</td>
</tr>
<tr>
<td>Excess Temperature</td>
<td>Compressor valve failure&lt;br&gt;Cooler failure&lt;br&gt;Excess compression ratio&lt;br&gt;Insufficient flow</td>
<td>High Temperature</td>
</tr>
</tbody>
</table>
Example Safety Analysis Checklist

Table A-1.2—Safety Analysis Checklist (SAC)—Flow Line Segment

a. High Pressure Sensor (PSH).
1. PSH installed.
2. Flow line segment has a maximum allowable working pressure greater than maximum shut in pressure and is protected by a PSH on a downstream flow line segment.

c. Pressure Safety Valve (PSV).
1. PSV installed.
2. Flow line segment has a maximum allowable working pressure greater than the maximum shut in pressure.
3. Two SDVs (one of which may be the SSV) with independent PSHs, relays, and sensing points are installed where there is adequate flow line volume upstream of any block valves to allow sufficient time for the SDVs to close before exceeding the maximum allowable working pressure.
4. Flow line segment is protected by a PSV on upstream segment.
5. Flow line segment is protected by a PSV on downstream component that cannot be isolated from the Flow line segment and there are no chokes or other restrictions between the Flow line segment and the PSV.
Location of safety systems according to API 14C

Figure A-8—Recommended Safety Devices—Compressor Unit

Notes:
1. TSE designations are symbolic and are not intended to reflect actual location or quantity.
2. ASH 1, 2 & OSH 1, 2 are not required if compressor is not installed in an enclosed building.
3. ASH 3 is not required if compressor does not have piping or other potential source of gas leak below a solid subfloor.
4. Suction scrubbers are not shown; they should be analyzed according to Section A.4.
5. OSH 1 should be considered based on the conditions stated in Appendix F, Parameters F-1.1 and F-1.2.
6. Shell-tube type discharge coolers are not shown; they should be analyzed according to section A.10.
Survivability
Can our Safety Barrier fulfill its function under accident Conditions?

Jet fire Thermal radiation

UCVCE Blast Overpressure
Performance Standard

Performance standards are prepared to summarise the following requirements for the safety critical system, subsystems and elements with a traceable and auditable manner:

- Goals
- Boundaries
- Functionalities
- Reliability / Availability
- Survivability
- Interaction / Dependences.

Verification schemes define the risk based inspection to ensure that the performance standards are maintained during operation (Fig-7).
# Performance Standard Tables

<table>
<thead>
<tr>
<th>Performance Objectives:</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Components:</td>
</tr>
</tbody>
</table>

## Functionality
- **Function**: Performance Criteria & Basis
- **Assurance**: Verification

## Reliability / Availability
- **Sub-System/Component**: Performance Criteria & Basis
- **Assurance**: Verification

## Survivability
- **Hazardous Event**: Performance Criteria & Basis
- **Assurance**: Verification

## Interactions / Dependencies / Limitations
- **System/Sub-System**
- **Supplier**: Safety Critical Element (Y/N)
- **Interactions/Dependencies/Limitations**: Performance Standard Ref.
- **Responsibility**

## Integrity Envelope
- **Failure Mode**: Performance Criteria Threshold
- **Operational Limitation**

## Safety Critical Elements (Equipment, Components and Software)
- **Element**
- **Supplier**
- **Failure Mode**
- **Severity Ranking**
- **Assurance**: Verification
HAZOP

Dynamic Simulation for an objective
Consequence analysis
OTS High Fidelity Dynamic Simulation

(Demo: http://www.adepp.com/Site_Demo/ADEPP_HSE_Toolkit.html)
Laplace Transform & Dynamic Simulation

With permission and courtesy of Ventimar LLC and SimApp
Full report is available @ http://www.simapp.com/simulation-tutorials
ADEPP Monitor
A tool for Life cycle LOPA
ADEPP LOPA monitor combines the followings to cover the life cycle issues of the required layers of protection:

- Dynamic & Knowledge based HAZOPs
- BPCS Control strategy
- Alarm Management Analysis
- API 14C
- SIL Assessment
- Fire & Explosion study
- Performance Standards
- Verification Schemes

Both **Code based** and **Risk based** are used in ADEPP LOPA monitor.
ADEPP LOPA monitor

(Demo: http://www.adepp.com/Site_Demo/ADEPP_HSE_Toolkit.html)
Thank you for your kind attention!

For more information contact: fabienne@adepp.com